Herramienta para soporte de la Administración del Riesgo en TI Apoyado en la Metodología AUDAP

MARIO ADRIÁN GONZÁLEZ COMAS 72023021

TOMAS ENRIQUE PALMA GUZMÁN 72020292

UNIVERSIDAD DE LA COSTA – CUC

ESPECIALIZACION DE AUDITORIA DE SISTEMAS DE INFORMACION

BARRANQUILLA

2012

Herramienta para soporte de la Administración del Riesgo en TI Apoyado en la Metodología AUDAP

Mario Adrián González Comas

Tomas Enrique Palma Guzmán

MONOGRAFÍA PARA OPTAR AL TITULO DE AUDITOR DE SISTEMASDE INFORMACION

UNIVERSIDAD DE LA COSTA

ESPECIALIZACION DE AUDITORIA DE SISTEMAS DE INFORMACION

BARRANQUILLA

2012

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

RESUMEN

Ofrecer a los profesionales que se desempeñan en el área de la administración de riesgos, una herramienta de gestión para esta disciplina, apoyada en la metodología AUDAP como proceso que permite la identificación de los riesgos en el área de TI y en el estándar AS/NZ 4360 de administración de riesgos.

Obteniendo como resultado un software que permite al usuario un mayor entendimiento y facilidad en l a organización de riesgos, controles y tratamientos, aplicados en la gestión. Así como también permite la creación y planificación de actividades y el registro de las evidencias recolectadas durante el proceso.

SUMARY

Providing professionals who work in the area of risk management, a management tool for the discipline, based on the methodology and process AUDAP allowing identification of risks in the IT area and in the standard AS / NZ risk Management 4360.

Resulting in software that allows the user a greater understanding and ease in organizing risks, controls and treatments, applied in management. And also allows the creation and planning of activities and registration of the evidence collected during the process.

TABLA DE CONTENIDO

INTRODUCCION

En la actualidad en diversas organizaciones se visiona y se evidencia el éxito, gracias al aprovechamiento de los beneficios que trae el área de TI, pues esta ofrece eficiencia y agilidad en los procesos, entrega oportuna y confiable de la información para la toma de decisiones, dentro de toda organización de calidad se aplica la estrategia de ayudar en las acciones para la consecución de sus objetivos.

La administración de los riesgos no es más que el estudio, prevención y manejo de los riesgos presentes en entidades, negocios y grandes empresas. Ahora bien esta administración de riesgo se ha podido venir dando de una u otra manera, pero se debe buscar la forma más adecuada para el manejo de los riesgos, esto con el fin de lograr de manera eficiente el cumplimiento de los objetivos de la organización.

La organización debe entender que TI no es un área aislada sino que esta debe ser convertirse en parte integral del manejo total de una empresa; es decir, la TI necesita ser adoptada como parte integral de la empresa, en lugar de concebirse como algo que se practica en un rincón aislado o como simple teoría.

Ahora bien la administración del riesgo de TI debe ser un proceso el cual se aplica y se mantiene, por lo tanto se debe evaluar constantemente los controles aplicados y determinar si estos son los adecuados para la mitigación de los riesgos presentes, de esta manera obtener bases más confiables para la planeación y toma de decisiones en el área de TI, identificar las oportunidades de TI así como las amenazas, asignar y usar de manera más efectiva los recursos, aumentar la confianza de los inversionistas.

El proceso de la administración del riesgo debe ser debidamente sustentado y documentado, para realizar la adecuada toma de decisiones con respecto a los

controles que se implementan para la mitigación de los riesgos, esto se consigue con un monitoreo constante.

Lo anteriormente dicho es resultado de la concepción de la administración de los riesgos, lo cual busca la consecución de los objetivos de la organización a través de la mitigación de los riesgos existentes dentro de las organizaciones y en el área de TI.

Los anteriores interrogantes tendrán respuesta con el desarrollo de esta investigación.

OBJETIVO GENERAL

Ofrecer a los profesionales que se desempeñan en el área de la administración del riesgo una herramienta de gestión para esta disciplina, apoyándose en la metodología ADUDAP como proceso que permite la identificación de los riesgos en el área de TI, y en el estándar AS/NZS 4360.

OBJETIVOS ESPECIFICOS

- Utilizar el estándar AS/NZS4360 utilizando la metodología AUDAP para facilitar un desempeño eficiente en el área de administración de riesgos.

- Desarrollar un software para dar soporte a la aplicación del estándar 4360 dentro del área de administración de riesgos.

- Implementar el estándar AS/NZS 4360 en conjunto con la metodología AUDAP para facilitar toda acción en el área de administración de riesgo.

1. PLANTEAMIENTO DEL PROBLEMA

Durante la ejecución de un proyecto de la gestión del riesgo que se desea implementar dentro de una empresa, siempre es necesario llevar la documentación de los avances, evidencias y actividades que se llevan acabo.

Uno de los inconvenientes que más se presenta, es la ausencia de un método organizativo para llevar la documentación de los riesgos, evaluaciones, controles y actividades realizadas durante la implementación de la gestión del riesgo, y que permita el fácil acceso a esta información.

Tal inconveniente es solventado mediante el uso de herramientas o metodologías asistidas por computador, las cuales ofrecen un mejor desempeño y accesibilidad a la información de la gestión que se esta llevando a cabo.

Este proyecto ofrece como solución un software que permitirá el ingreso de la información que se recolecta durante la ejecución de la gestión del riesgo, llevarla de una manera organizada y así mismo tener acceso a esta de manera eficiente.

El software combinara la metodología asistida por computador y el estándar de la gestión del riesgo AS/NZ 4360.

2. JUSTIFICACION E IMPORTANCIA DEL PROYECTO

En la actualidad la administración de los riesgos es fundamental en el proceso de consecución de los objetivos del negocio, de ahí que el proyecto que se desea realizar, encuentra su justificación en el desarrollo de una herramienta que permita, soportar el proceso de la administración de los riesgos y utilizar la metodología AUDAP para la identificación de los mismos en el área de TI y obtener de manera oportuna y confiable la información relacionada a este proceso.

El presente estudio busca el desarrollo de una herramienta que permita la gestión del proceso de administración de riesgos, apoyándose en la metodología ADUDAP para la identificación de los riesgos en el área de TI, ya que por medio de su implementación se generaría información útil para la toma de decisiones y de aplicación de controles para la mitigación de riesgos y monitoreo de los controles aplicados, esta manera estar preparados ante alguna contingencia que se presente.

Uno de los constantes inconvenientes con el desarrollo de un proyecto de gestión de riesgos, es el manejo de los papeles de trabajo, acopio de evidencias y la definición de actividades de auditoria y monitoreo, estos inconvenientes pueden verse facilitados y mejorados mediante el uso de un software como herramienta de apoyo durante la implementación de la gestión de riesgo, el cual podrá proveer una base de conocimiento de los riesgos existentes, a los cuales se podrá tener acceso para la identificación de los riesgos en la organización en la cual se esté trabajando, visualizar la evaluación de riesgos mediante el uso de matrices de riesgos, creación y programación de actividades de monitoreo, así como la asignación de evidencias recolectadas durante la ejecución de estas, permitiendo de esta manera tener acceso a las evidencias de una manera rápida y eficiente.

3. DISEÑO METODOLOGICO

3.1. Tipo de investigación

El enfoque de la investigación es aplicada dado que con el desarrollo de esta se obtener el desarrollo de una aplicación la cual pueda ser utilizada para cubrir las necesidad de mejorar el proceso de gestión del riesgo, es decir que se organizaran los conceptos relacionados con la gestión del riesgo, se priorizaran, se planificara y desarrollara una aplicación para este fin.

Dado el carácter y esencia de la investigación se puede decir que la investigación tiene un enfoque cualitativo, dado que durante el desarrollo de esta, se realiza un estudio analítico y deductivo de las características y etapas que comprenden la implementación de un sistema de gestión de riesgos, y basados en esto diseñar y desarrollar una aplicación que soporte dicho sistema de gestión de riesgos.

3.2. Fuentes de información

Para el desarrollo de la metodología, se utilizo la técnica de recolección de información secundaria, centrándose en referencias bibliográficas sobre el estándar de análisis y gestión de riesgos AS/NZ 4360, y técnicas de auditorias asistidas por computador AUDAP.

Para la recolección de la información necesaria para el desarrollo de la herramienta, se realizara una investigación del material existente sobre estándares de administración de riesgos y metodologías asistidas por computador.

Esta información se obtendrá de la documentación existente sobre el estándar AS/NZ 4360 para la administración del riesgo, tales como documento oficial del estándar y metodología utilizada para la implementación de este estándar. También se aplicara este mismo tipo de recolección de datos para la información existente de la metodología asistida por computador AUDAP.

Se escoge estas dos metodologías dada su amplia aceptación e implementación.

4. RESULTADOS ESPERADOS

Como resultado de esta investigación, se desarrollara un aplicación la cual será utilizada como herramienta y técnica asistida por computadordurante la implementación de la gestión de riesgo, el cual podrá proveerá una base de conocimiento de los riesgos existentes, a los cuales se podrá tener acceso para la identificación de los riesgos en la organización en la cual se esté trabajando y así mismo poder ir alimentando esta a lo largo de la ejecución de la gestión del riesgo, permitiendo una mayor definición en el universo de riesgos, para futuros proyectos de implementación, permitirá visualizar la evaluación de riesgos mediante el uso de matrices de riesgos, facilitara la creación y programación de actividades de monitoreo, así como la asignación de evidencias recolectadas durante la ejecución de estas, permitiendo de esta manera tener acceso a las evidencias de una manera rápida y eficiente.

Todo esto con el fin de agilizar el acceso de la información que se ha recolectado, permitiendo que la información sea transparente y fluida

5. MARCO TEORICO

5.1. ESTANDAR AS/NZ 4360

En la actualidad las empresas son conscientes de la necesidad de realizar una gestión al riesgo algunas empresas desarrollan esta gestión de una forma Autónoma, pero existen estándares que ayudan a la administración del riesgo, tal es el caso de la AS/NZS 4360 El estándar **AS/NZ: 4360** es el único estándar de uso mundial para la administración del riesgo puro. Desarrollado por las oficinas de estándares de Australia y Nueva Zelanda. Ha sido adoptado por todo tipo de entidades del estado y del sector privado en todo el mundo. Este estándar está **alineado** con normas y estándares mundiales y locales de gestión del riesgo tales como: Basilea, Ley SOX, MECI, Guía de gestión del Riesgo del DAFP y otros. Que es el estándar australiano este suministra orientaciones genéricas para la gestión de riesgos. Puede aplicarse a una gran variedad de actividades, decisiones u operaciones de cualquier entidad pública, privada o comunitaria, grupos o individuos. Se trata de una instrucción amplia pero que permite la definición de objetivos específicos de acuerdo con las necesidades de cada implementación.

Trae los siguientes Beneficios a la empresa:

- Estandarización de la práctica de gestión de riesgos entre las diversas áreas de la empresa.
- Implantación de mecanismos de evaluación de riesgos y revisión de procesos.
- Implantación de mecanismos de control y tratamiento.
- Reducción de riesgos para los procesos corporativos.
- Reducción de costos provenientes de los riesgos.

Además de estos beneficios, la aplicación de la norma AS/NZS 4360 le garantiza a la organización una base sólida para la aplicación de cualquier otra norma o metodología de gestión de riesgos específica para un determinado segmento.

5.2 Definiciones.

Para el propósito de estándar se aplican las siguientes definiciones:

Consecuencia

El resultado de un evento expresado en forma cualitativa o cuantitativa, que genera pérdida, daño, desventaja o ganancia. Estos pueden ser un rango de posibles resultados asociados con el evento.

Costo

De una actividad, tanto directa como indirecta, involucran un impacto negativo, incluyendo dinero, tiempo, trabajo, interrupción, goodwill, pérdidas políticas e intangibles.

Evento

Un incidente o suceso, el cual ocurre en un determinado lugar durante un determinado intervalo de tiempo.

Árbol de análisis de causas.

Es una técnica que describe el posible rango y secuencia los resultados que pueden originarse de un evento inicial.

Análisis de Modos de fallas y efectos – Failuremode and effectsanalysis (FMEA)

Es un procedimiento mediante el cual los modos potenciales de fallas en un sistema técnico son analizados.

Árbol de análisis de fallas

Es un método de ingeniería de sistemas que representa la combinación lógica de varios estados del sistema y de las posibles causas que pueden contribuir a un evento específico. (Llamado el evento de mayor nivel).

Frecuencia

Es una medida sobre la rata de ocurrencia de un evento expresado por el número de ocurrencias de un evento en un tiempo dado. Ver también probabilidad.

Amenaza

La fuente de daño potencial o una situación que potencialmente cause pérdidas.

Probabilidad

Se usa como una descripción cualitativa de la probabilidad o la frecuencia.

Pérdida

Una consecuencia negativa, financiera o de cualquier otra índole.

Monitoreo

Verificar, supervisar, observar o registrar el progreso de una actividad, acción o sistema sobre una base regular, con el fin de **identificar cambios**.

Organización

Una compañía, firma, empresa o asociación, u otra entidad de tipo legal o de cualquier índole, esto es incorporada o no, pública o privada, que tiene sus propias función y administración.

Probabilidad

La posibilidad que un evento específico o resultado, medido por la rata de eventos específicos o resultados dentro de un número total de posibles eventos o resultados. La Probabilidad es expresada como un número entre 0 y 1, en donde cero indica que es imposible que el hecho ocurra y 1 indica que el evento es cierto.

Riesgo residual

Se refiere al margen o residuo de riesgo que puede darse a pesar de las medidas de tratamiento tomadas para la administración del riesgo.

Riesgo

La posibilidad que algo suceda y que podría tener un impacto sobre los objetivos. Está medido en términos de consecuencias y probabilidad de ocurrencia.

Aceptación del riesgo

Es la decisión informada de aceptar las consecuencias y la probabilidad de un riesgo particular.

Análisis del riesgo

El uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.

Valoración del riesgo.

El conjunto de procesos para analizar y evaluar el riesgo

Evitar el riesgo.

Decisión informada de no involucrarse en una situación de riesgo.

Control del Riesgo

Se refiere a la parte de la administración de riesgo, que involucra la implantación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

Ingeniería de riesgos

Es la aplicación de principios y métodos de ingeniería para la administración del riesgo.

Evaluación del riesgo

El proceso utilizado para determinar prioridades en la administración del riesgo por la comparación de niveles de riesgo frente a estándares determinados, limites de niveles del riesgo u otros criterios.

Financiación el riesgo

Los métodos aplicados para financiar la administración del riesgo y las consecuencias financieras del riesgo.

Identificación del riesgo.

Proceso para determinar **QUE** puede suceder, **POR QUE** y **COMO**.

Administración del riesgo

La cultura, los procesos y las estructuras que están dirigidas hacia una efectiva administración de potenciales **oportunidades** y **efectos adversos**.

Proceso de Administración del Riesgo

La aplicación sistemática de políticas gerenciales, procedimientos y prácticas, en las actividades para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos.

Reducción del riesgo

La aplicación selectiva de técnicas apropiadas y principios gerenciales para reducir la **probabilidad** de ocurrencia de un evento o sus **consecuencias** o **ambos**.

Retención (conservación) del riesgo

Intencionalmente o no, conservar la responsabilidad por pérdidas o provisiones para pérdidas, al interior de la empresa.

Transferir el riesgo

Transferir total o parcialmente la responsabilidad de la provisión para pérdidas a un tercero a través de la ley, contratos, seguros u otro medio. Transferir el riesgo puede también hacer referencia a mover físicamente el riesgo o parte del mismo a otro sitio.

Tratamiento del riesgo (Administración del riesgo)

Seleccionar e implementar las opciones apropiadas para reducir el riesgo.

Análisis de sensibilidad

Examinar cómo los resultados del cálculo de un modelo varían cuando los supuestos individuales son modificados.

Stakeholders (Objetos del riesgo, los que toman el riesgo)

Son las personas y las organizaciones quienes pueden ser afectadas, son afectadas por, o perciben que ellos mismos pueden ser afectados por una decisión o actividad.

5.3. METODOLOGIA MAGERIT

Esta es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, **MAGERIT** les permitirá saber cuánto valor

está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con **MAGERIT** se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

5.4. ADMINISTRACION DE RIESGO

Es el proceso por el cual la dirección de una empresa u organización administra el amplio espectro de los riesgos a los cuales está expuesto (tanto sean de mercado como operacionales) de acuerdo al nivel de riesgo al cual están dispuestos a exponerse según sus objetivos estratégicos. Así, ya en el terreno del impacto de la TI sobre este tema, la evaluación de riesgos y vulnerabilidades ayuda a identificar y evaluar los riesgos operativos, poniendo énfasis en los activos de IT físicos y lógicos, pudiendo incluir una revisión de las instalaciones y la seguridad de los elementos lógicos y físicos.

Permite identificar los activos que están en máximo riesgo, evaluar las vulnerabilidades y los impactos potenciales, y proponer resguardos y tácticas de mitigación, lo que permitirá:

Permite identificarlos recursos empresariales que están en mayor riesgo, evaluar las vulnerabilidades y los impactos potenciales y proponer tácticas de mitigación.

Priorizar y establecer niveles de riesgo para sus procesos y recursos críticos.

Pasar de un enfoque de mitigar el riesgo a prevenir las fallas.

Evaluar las tácticas y los costos de la administración de los riesgos con los diferentes niveles de protección.

Evaluar las tácticas y los costos de la administración de riesgo relacionados con los diferentes niveles de protección.

Problemas que se atacan

- Identificar eventos o amenazas que podrían tener impacto en la continuidad de las operaciones empresariales, en la imagen o en la reputación de la marca, y la probabilidad de que ocurran.
- Realizar un análisis detallado de amenazas o establecer planes de avance para mitigar riesgos.
- Determinar como las nuevas iniciativas empresariales o la nueva tecnología tendrá impacto en la empresa.

5.5. METODOLOGÍA AUDAP

Es la metodología asistida por computador, desarrollada para conducir auditorías orientadas al riesgo en operaciones automatizadas

Desarrolla auditorías integrales de la Seguridad de la información y el Control Interno:

- **Controles Automatizados** - Implementados y ejecutados en el software aplicativo y del sistema.
- **Controles No Automatizados.** Implementados en los procedimientos ejecutados por personas en las áreas de operación del negocio o servicio.

Esta metodología cuenta con herramientas para la gestión de la auditoria basara en riesgos un ejemplo es **AUDPA/AUDIRISK**, este se encuentra en la Versión 2009, desarrollada por AUDISIS LTDA. (Colombia) El software AUDAP (AUDIRISK, a partir del año 2010) es una herramienta para apoyar a auditores internos, externos y de sistemas en el desarrollo de "AUDITORÍAS

BASADAS EN RIESGOS" a los procesos del modelo de operación de la Empresa (estratégicos, misionales, de apoyo y de evaluación), procesos de tecnología de información (modelos COBIT, ITIL), Aplicaciones de Computador (o módulos de ERPs) y el seguimiento a los planes de mejoramiento institucional que surgen de auditorías internas y externas realizadas en la organización.

Otra de las herramientas desarrolladas para dar soporte a la administración del riesgo es **RISK Advisor**, el cual es una herramienta, que asiste al usuario paso a paso para implementar un Sistema de Administración Integral del riesgo (**SAIR**), en todos sus procesos, proyectos u otras actividades críticas para el logro de sus objetivos y metas estratégicas. Permite identificar el nivel real de exposición de su organización y generar diversos Mapas de Riesgos a diferentes niveles.

Esta herramienta esta basada en el estándar de administración del Riesgo AS/NZS: 4360 y la NTC 5254 - Norma Técnica Colombiana de “Gestión del Riesgo” ICONTEC-2004, que provee una metodología y guía genérica, para la implementación del proceso de gestión del riesgo considerando todas sus etapas: Entender el contexto, identificar, analizar, valorar, tratar y monitorear todos los riesgos que puedan afectar los objetivos y metas de su organización.

6. ESTADO DEL ARTE

En la actualidad se han desarrollado un gran número de herramientas para soportar procesos de gestión de riesgos y auditorias basadas en riesgos, cada una de estas herramientas ofrecen a los usuarios diferentes formas y enfoques para identificar, analizar, evaluar y tratar los riesgos, y así mismo formas y mecanismos para realizar las debidas actividades de auditoría y de esta forma poder llevar una buena documentación y monitoreo sobre esos mismos riesgos.

Durante el desarrollo de este proyecto se realizo una investigación sobre que software para gestión de riesgos existen en el mercado de los cuales se escogieron los que aparecen en la siguiente lista, dada su afinidad al lineamiento que se le ha dado al desarrollo del software:

- ControlRisk
- AudiRisk
- ORCA GRC Suite
- CERO – Control Estratégico de Riesgo
- RiskAdvisor

A continuación se da una breve descripción de cada uno de las herramientas mencionadas

AUDIRISK

Es una herramienta desarrollada por AUDISIS LTDA, Auditoría Integral y Seguridad de Sistemas de Información Ltda., es una firma de Auditores – Consultores Gerenciales, constituida legalmente el 23 de Septiembre de 1.988.

Audirisk es un software en tecnología web para desarrollar auditorias basadas en riesgos y efectuar seguimiento a los hallazgos de auditorías efectuadas por terceros, Audirisk estandariza el desarrollo de las auditorias de la empresa en una sola aplicación y en una única base de datos con los papeles de trabajo de todas las auditorias, alineadas con las normas y procedimientos de auditorías generalmente aceptados y con estándares nacionales e internacionales de administración de riesgos.

CONTROLRISK

Es una herramienta desarrollada por AUDISIS LTDA, Auditoría Integral y Seguridad de Sistemas de Información Ltda., es una firma de Auditores – Consultores Gerenciales, constituida legalmente el 23 de Septiembre de 1.988.

ControlRisk es un software en tecnología web que soporta la implementación, mantenimiento y actualización del sistema de administración integral de riesgos (SAIR) de la empresa. Provee funcionalidades para desarrollar el ciclo PHVA de la gestión del riesgo por procesos, alineando con las normas y procedimientos de auditorías generalmente aceptados y con estándares nacionales e internacionales de administración de riesgos y diseño de controles.

ORCA GRC Suite

ORCA por sus siglas en ingles (OrganizationalRisk and ComplianceAdministration) es una solución de administración de riesgos, cumplimiento y gobierno corporativo, que ayuda a centralizar, analizar y comprender los riesgos asociados con los procesos de negocio críticos, optimizando la seguridad y los niveles de cumplimiento, brindando a los tomadores de decisiones una experiencia única a través de los tableros de control con inteligencia en información GRC.

CERO – Control Estratégico de Riesgo

CERO es el software creado por PRAGMA, que permite la gestión y control de los riesgos

Enlamedidaenquelasorganizacionesalcanzanunmayorgradodemadurez,sehacenconscientesdelanecesidaddegestionarlosriesgosafindereducirelimpactoquecausanylafrecuenciadedichosriesgosyasípoderminimizarlaspérdidasasociadasadichasmaterializaciones.CEROfuecreadoconelfindecubrirelprocesodegestiónderiesgosdeunamaneraestructuradaysistematizada,yapoyarlosprocesosqueseejecutanalrededordedichagestión.

RISK ADVISOR

El RiskAdvisor es una herramienta, que asiste paso a paso la implementación del Sistema de Administración Integral del riesgo (SAIR) dentro de una organización, en todos sus procesos, proyectos u otras actividades críticas para el logro de sus objetivos y metas estratégicas. Permite identificar el nivel real de exposición de una organización y generar diversos Mapas de Riesgos a diferentes niveles.

RiskAdvisorestá basado en el estándar de administración del Riesgo AS/NZS: 4360 y la NTC 5254 - Norma Técnica Colombiana de “Gestión del Riesgo”

ICONTEC-2004, que provee una metodología y guía genérica, para la implementación del proceso de gestión del riesgo considerando todas sus etapas: Entender el contexto, identificar, analizar, valorar, tratar y monitorear todos los riesgos que puedan afectar los objetivos y metas de su organización.

7. MANUAL DEL SISTEMA

7.1. Requerimientos de la aplicación

El software a desarrollar soportara el proceso de gestión del riesgo teniendo como base el estándar AS/NZ 4360, permitiendo de esta manera que el usuario pueda ingresar los riesgos, la aplicación se orientada a web, para facilitar el acceso del usuario

Requerimientos funcionales

Entre los requerimientos funcionales de la aplicación tenemos:

- tener como base el estándar AS/NZ 4360 para gestión de riesgos
- deberá poder manejar más de una empresa y poder cambiar de empresa cada vez que el usuario lo desee.
- soportar más de un usuario y asignarlos por empresa
- definición de variables para controles, tratamientos y eventos por parte de los usuarios
- base de conocimiento para riesgos
- manejo de reportes
- en la evaluación de riesgos deberá mostrar los que han sido evaluados y los que no aun faltan por evaluar
- creación, programación de actividades
- guardado de evidencias escaneadas en formado bmp, jpg, png

Requerimientos no funcionales

- la aplicación debe ejecutarse en el navegador Internet Explorer
- motor de base de datos MySQL

7.2. Características Generales

En este ítem se dan a conocer las características generales con las cuales cuenta el software desarrollado para la gestión del riesgo; características como sistemas operativos en los que se puede ejecutar el software, lenguaje de programación, gestor de base de datos y el sistema de infraestructura de internet, el cual es utilizado para dar soporte y funcionamiento al software dado que este se encuentra orientado a web

Sistemas operativos: el software es compatible con las versiones de Windows 95/98, Windows Vista, Windows 7

Lenguaje de Desarrollo: PHP 5.2.4

Gestor Base de Datos: MySQL 5.0.45-community-nt

Sistema de Infraestructura Internet: WAMP

7.3. Manual de Instalación

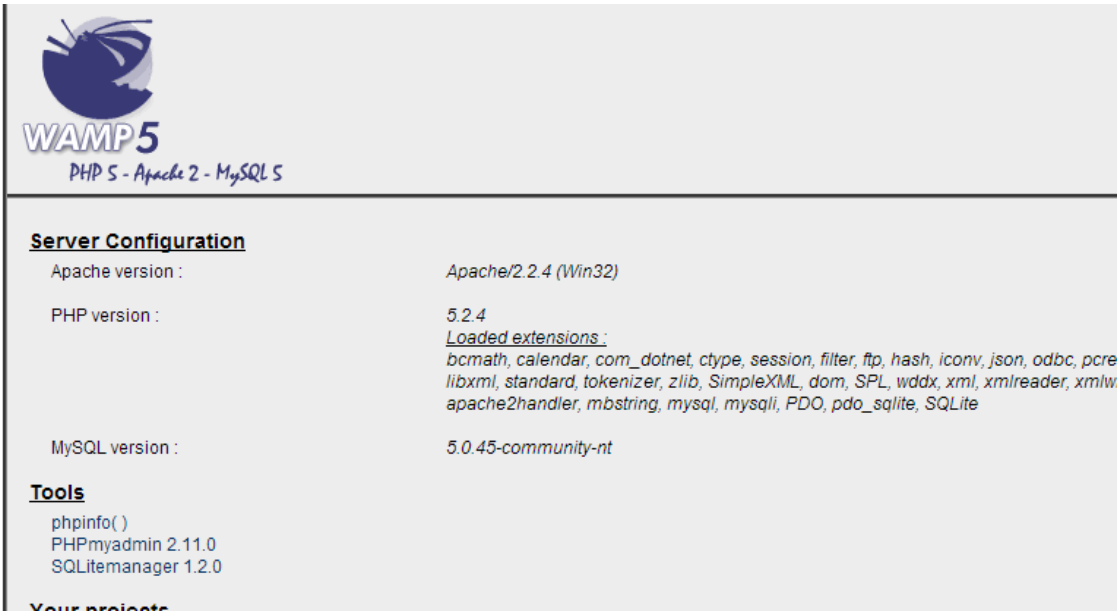
El siguiente es el manual para la instalación del software orientado a web CUC-AUDITRISK, este manual le guiara paso a paso a la instalación del software

Creación de la base de datos

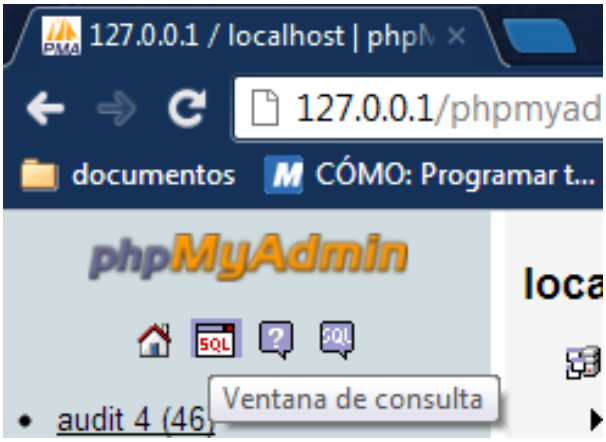
Antes de la creación de la base de datos del CUC – Auditrisk, debemos instalar el motor de base de datos y las librerías necesarias para el correcto funcionamiento del software.

En primera instancia se instalara el WAMP el cual se encargara de la administración de la Base de Datos, conexión entre la aplicación y la base de datos y librerías de funcionamiento, el cual encontraremos en la ruta /Utilidades, procederemos con la instalación del WAMP, una vez instalado se procederá con la creación de la base de datos

Para la creación de la base de datos se deberá abrir el archivo “Código SQL Base de Datos CUC RISKAUDIT.txt” el cual se encuentra en el CD en la ruta /software, copiaremos el código y en un navegador de internet digitaremos la dirección 127.0.0.1 la cual pertenece al localhost en donde instalaremos el software



Una vez encontremos la página que vemos en la imagen anterior, procederemos a seleccionar la OpciónPHPmyadmin, y escogeremos la opción de consultas para la ejecución del código SQL



Copiaremos y pegaremos el código de la consulta y daremos clic en continuar, con esto habremos creado la base de datos de CUC-Auditrisk

Para la instalación de la página de navegación solo tenemos que copiar la carpeta que se encuentra en /Software la cual tiene el nombre de CUC AuditRisk, este contenido lo pegaremos en la siguiente dirección C:\wamp\www, una vez realizado esto, podemos ejecutar el acceso a CUC – AUDITRISK, el cual contiene un acceso directo en la carpeta software

7.4. Plataforma Base de Datos

MySQL es un Sistema de gestión de base de datos relacional, multiusuario, dada las características del software a desarrollar, el cual es orientado a web se escoge este motor de base de datos, dada su versatilidad para el manejo de usuarios y compatibilidad con la infraestructura de internet WAMP

7.5. Diccionario De Datos

tbl_acept_risk

Comentarios de la tabla: listado riesgos aceptados; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_risk	varchar(45)	No		código de identificación asignado al riesgo
motiv_acept	varchar(255)	No		motivo por el cual el riesgo es aceptado con su nivel de severidad
etap_acept	varchar(80)	No		etapa en la cual se acepta el riesgo

tbl_amenazas

Comentarios de la tabla: InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
amenaza	varchar(255)	No		

tbl_aproc_pcobit

Comentarios de la tabla: asignación de procesos de la empresa a procesos cobit; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_proc	varchar(45)	No		
id_pcobit	varchar(45)	No		

tbl_area_emp

Comentarios de la tabla: Descripción de las áreas que conforman la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
id_area	varchar(45)	No		
nomb_area	varchar(60)	No		
descrip_area	varchar(255)	No		

tbl_areaimpact

Comentarios de la tabla: Descripción de las áreas de impacto de la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_proc	varchar(45)	No		
id_ai	varchar(45)	No		

nomb_ai	varchar(60)	No		
Descrip_ai	varchar(255)	No		

tbl_calendar_activ Comentarios de la tabla: calendario de actividades para realizar monitoreo; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_prog	varchar(45)	No		código de programación actividad
fecha_activ	date	No		fecha en la cual se llevo a cabo la actividad
descrip_active	varchar(255)	No		descripción de la actividad llevada a cabo
Responsable	varchar(80)	No		nombre del responsable de llevar a cabo la actividad de monitoreo
Cargo	varchar(80)	No		cargo del responsable encargado de la ejecución de la actividad
estado_activ	varchar(90)	No		
Resultados	varchar(255)	No		
Conclusiones	varchar(255)	No		

observaciones	varchar(255)	No		este campo se registran las observaciones que tenga el auditor o la persona que llevo a cabo la actividad

tbl_clasf_ctrl

Comentarios de la tabla: clasificación del control según su tipo; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_ctrl	varchar(45)	No		
prev_ctrl	varchar(90)	No		
detec_ctrl	varchar(90)	No		
correct_ctrl	varchar(90)	No		

tbl_controles

Comentarios de la tabla: Descripción de los controles utilizados por procesos; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_ctrl	varchar(45)	No		identificación del control (código
nomb_ctrl	varchar(90)	No		nombre del control
desc_ctrl	varchar(255)	No		descripción del control
Categoría	varchar(50)	No		categoría del control

frec_ctrl	varchar(50)	No		frecuencia del control
Complejidad	varchar(50)	No		complejidad del control
Cobertura	varchar(60)	No		cobertura del control
Reponsables	varchar(60)	No		responsables del control
Acción	varchar(45)	No		sobre que actúa el control probabilidad o impacto

tbl_crea_activ

Comentarios de la tabla: esta tabla manejara los datos de creación de las actividades; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
id_activ	varchar(45)	No		código que identifica la actividad
nomb_activ	varchar(255)	No		nombre de la actividad
obj_activ	varchar(255)	No		objetivo de la actividad
descrip_active	varchar(255)	No		
frec_activ	varchar(60)	No		frecuencia con que se ejecutara la actividad
Fecha	date	No		fecha en que se crea la

				actividad

tbl_crit_consec

Comentarios de la tabla: Descripción de los criterio de consecuencias utilizados por; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
id_crit_consec	varchar(45)	No		
nomb_crite	varchar(255)	No		
desc_rechuma	varchar(255)	No		
desc_perdi_econo	varchar(255)	No		
desc_perd_repu	varchar(255)	No		
Valor	varchar(12)	No		

tbl_crit_info

Comentarios de la tabla: información de criterios de la información establecidos por;InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_crit_info	varchar(45)	No		
nomb_crit_info	varchar(90)	No		
desc_crit_info	varchar(255)	No		

tbl_crit_prob

Comentarios de la tabla: Descripción de los criterios utilizados por la empresa para;InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
id_crit_prob	varchar(45)	No		
nomb_crit_prob	varchar(255)	No		
desc_posi_b	varchar(255)	No		
desc_posi_mat	varchar(255)	No		
desc_frec	varchar(255)	No		
Valor	varchar(12)	No		

tbl_debiliades

Comentarios de la tabla: Descripción de Debilidades Matriz DOFA; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
debilidad	varchar(255)	No		

tbl_element_trata

Comentarios de la tabla: Descripción de los elementos del tratamiento; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_trata	varchar(45)	No		codigo que identifica el tratamiento al cual asignaremos los elementos
element_trata	varchar(120)	No		elemento asignado al tratamiento
descrip_element	varchar(255)	No		descripción de los elementos asignados a los tratamientos

tbl_empresa

Comentarios de la tabla: descripción de la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_usua	varchar(64)	No		código usuario que crea y trabajara la empresa
id_emp	varchar(45)	No		
nomb_emp	varchar(255)	No		
Visión	varchar(255)	No		
Misión	varchar(255)	No		
País	varchar(255)	No		
dir_emp	varchar(255)	No		

Tel	varchar(25)	No		

tbl_eva_ctrl

Comentarios de la tabla: evaluación del riesgo con controles

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
id_risk	varchar(45)	No		
Prob	varchar(90)	No		
consec	varchar(90)	No		
Nivel	varchar(90)	No		

tbl_eva_risk

Comentarios de la tabla: Evaluación del riesgo inherente; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
id_risk	varchar(45)	No		
prob_risk	varchar(90)	No		
consec_risk	varchar(90)	No		
niv_risk	varchar(90)	No		
puntaje	varchar(10)	No		

tbl_eva_trata

Comentarios de la tabla: evaluación del riesgo con tratamientos; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
id_trata	varchar(45)	No		
consec_trata	varchar(90)	No		
prob_trata	varchar(90)	No		
niv_risk_trata	varchar(90)	No		

tbl_event_risk

Comentarios de la tabla: descripción del riesgo materializado por evento; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_event	varchar(45)	No		
id_risk	varchar(45)	No		

tbl_eventos Comentarios de la tabla: historial de eventos presentados en la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_event	varchar(45)	No		
id_emp	varchar(45)	No		
fecha_event	date	No		
id_risk	varchar(45)	No		codigo del riesgo materializado durante el evento
nomb_event	varchar(60)	No		nombre asignado al evento
desc_event	varchar(255)	No		
observ_event	varchar(255)	No		observaciones realizadas por el auditor sobre el evento del riesgo materializado
perdida_evento	varchar(255)	No		
categ_event	varchar(255)	No		
impact_prim	varchar(255)	No		
Probabilidad	varchar(90)	No		
area_afectada	varchar(255)	No		área en la cual se dio el evento
proceso_afectado	varchar(255)	No		proceso en el cual se dio el

				evento

tbl_evidenicia

Comentarios de la tabla: guardado de evidencias auditorias; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
cod_formato	varchar(45)	No		
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
cod_prog	varchar(45)	No		
nombre_eve	varchar(60)	No		
desc_eve	varchar(255)	No		
Ruta	text	No		

tbl_fortalezas

Comentarios de la tabla: Descripción Fortalezas Matriz DOFA; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
fortalezas	varchar(255)	No		

tbl_fuentrisk

Comentarios de la tabla: Descripción de las fuentes del riesgo según los procesos que; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_proc	varchar(45)	No		
id_fr	varchar(45)	No		
nomb_fr	varchar(80)	No		
Descrip_fr	varchar(255)	No		descripción fuente de riesgo

tbl_metas

Comentarios de la tabla: descripción de las metas de la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
Metas	varchar(255)	No		

tbl_niv_severidad

Comentarios de la tabla: administra los niveles de severidad creados por el usuario; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios

id_emp	varchar(45)	No		codigo de la empresa
niv_severidad	varchar(60)	No		nombre de nivel de severidad
desc_niv_sev	varchar(255)	No		descripción del nivel de severidad

tbl_objetivos

Comentarios de la tabla: descripción de los objetivos de la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
objetivo	varchar(255)	No		

tbl_oportunidades

Comentarios de la tabla: Descripción Oportunidades Matriz DOFA; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
oportunidad	varchar(255)	No		

tbl_politicas

Comentarios de la tabla: descripción de las políticas de la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios

id_emp	varchar(45)	No		
politica	varchar(255)	No		

tbl_proc_cobit

Comentarios de la tabla: Descripción de los 34 procesos que maneja COBIT; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_proc_cobit	varchar(45)	No		
nomb_proc_cobit	varchar(90)	No		
desc_proc_cobit	varchar(255)	No		

tbl_procesos

Comentarios de la tabla: Descripción de los procesos internos de la empresa; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_area	varchar(45)	No		
id_proc	varchar(45)	No		
nomb_proc	varchar(60)	No		
descrip_proc	varchar(255)	No		

tbl_prog_activ

Comentarios de la tabla: en esta tabla se maneja los datos de programación de activad; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios

id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
id_prog	varchar(45)	No		codigo de identificación de programación
id_activ	varchar(45)	No		id de la actividad
id_area	varchar(45)	No		id del area en la cual se realizara la actividad
id_proc	varchar(45)	No		id del proceso en el cual se realizara la actividad
fecha_inicio	date	No		fecha en la cual iniciara la actividad
Reponsable	varchar(60)	No		responsable de llevar a cabo la actividad
Observacio	varchar(255)	No		observaciones a la actividad
Estado	varchar(60)	No		estado de la actividad programada

tbl_recursos

Comentarios de la tabla: Recursos de la Información establecidos por COBIT; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios

id_recu	varchar(45)	No		
nomb_recu	varchar(90)	No		
desc_recu	varchar(255)	No		

tbl_riesgos

Comentarios de la tabla: Descripción del riesgo según procesos; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_risk	varchar(45)	No		
nomb_risk	varchar(80)	No		

tbl_riesgos_ai

Comentarios de la tabla: relación de riesgos y las áreas de impacto que se ven afecta; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_risk	varchar(45)	No		codigo de identificación asignado al riesgo
id_ai	varchar(45)	No		codigo asignado al area de impacto

tbl_riesgos_fr

Comentarios de la tabla: relación de riesgos y las fuentes de riesgos que se ven afec; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios

id_risk	varchar(45)	No		codigo de identificación asignado al riesgo
id_fr	varchar(45)	No		codigo asignado a la fuente de riesgo

tbl_riesgos_qcp

Comentarios de la tabla: esta tabla relaciona un riesgo con los diferentes QUE's, COM; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
id_risk	varchar(45)	No		
Que	varchar(255)	No		
Como	varchar(255)	No		
porque	varchar(255)	No		

tbl_risk_crit_info

Comentarios de la tabla: criterios de información que son afectados por un riesgo; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_crit_info	varchar(45)	No		
id_risk	varchar(45)	No		

tbl_risk_ctrl

Comentarios de la tabla: asignación de controles a riesgos; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
id_risk	varchar(45)	No		
id_ctrl	varchar(45)	No		

tbl_risk_recu

Comentarios de la tabla: recursos de la información afectados por el riesgo; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_risk	varchar(45)	No		
id_recu	varchar(45)	No		

tbl_severidad

Comentarios de la tabla: descripción de los niveles de severidad del risksegún la em; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
id_crit_prob	varchar(45)	No		
id_crit_consec	varchar(45)	No		

Severidad	varchar(90)	No		
Puntaje	varchar(12)	No		

tbl_stacke_proc

Comentarios de la tabla: en esta tabla se relacionan los procesos con los stackehold; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_stacke	varchar(45)	No		codigo de identificaciónstackeholder
id_proc	varchar(45)	No		codigo de identificación del proceso

tbl_stackeholder

Comentarios de la tabla: datos referente a los stackeholder que se ven afectados InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		identificación de la empresa
id_stacke	varchar(45)	No		cidog asignado al stackeholder
nomb_stacke	varchar(255)	No		nombre del stackeholder
descrip_stacke	varchar(255)	No		descripción del stackeholder
tipo_stacke	varchar(60)	No		tipo de stackeholder

tbl_transf_risk

Comentarios de la tabla: listado de riesgos que son transferidos; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_risk	varchar(45)	No		codigo de identificación asignado al riesgo
transf_to	varchar(100)	No		a quien es transferido el riesgo
motiv_transf	varchar(255)	No		motivo por el riesgo es transferido

tbl_tratamientos

Comentarios de la tabla: descripción y datos de el tratamiento a utilizar; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		
id_trata	varchar(45)	No		
id_risk	varchar(45)	No		
id_cont	varchar(45)	No		
nomb_trata	varchar(90)	No		
cobertura_t	varchar(90)	No		
Efecto	varchar(90)	No		

Tipo	varchar(90)	No		
Estado	varchar(90)	No		
Prioridad	varchar(90)	No		
descrip_trata	varchar(255)	No		
prop_trata	varchar(90)	No		

tbl_usuarios

Comentarios de la tabla: datos de los usuario que tendrán acceso a la aplicación; InnoDB free: 9216 kB

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_usua	varchar(64)	No		identificación del usuario
nom_usua	varchar(64)	No		nombre usuario
ape_usua	varchar(64)	No		apellido usuario
tel_usua	varchar(12)	No		telefono usuario
dir_usua	varchar(64)	No		dirección usuario
Cargo	varchar(64)	No		cargo del usuario
Perfil	varchar(255)	No		perfil del usuario
pass_usua	varchar(12)	No		contraseña usuario

tbl_variables

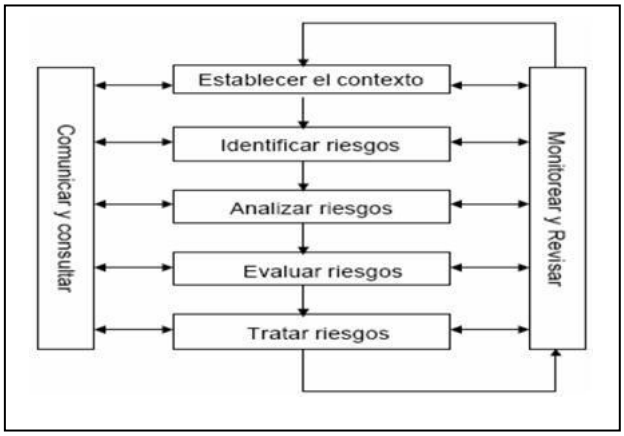
Comentarios de la tabla: en esta tabla se manejaran las variables con las cuales se e; InnoDB free: 9216

Campo	Tipo	Nulo	Predeterminado	Comentarios
id_emp	varchar(45)	No		codigo de la empresa en la cual se esta trabajando
eva_car	varchar(64)	No		evaluador al que pertenecerán las categorías
var_cat	varchar(64)	No		variable que sera alimentada

8. MANUAL DEL USUARIO

Es una herramienta que ofrece apoyo en el proceso de la gestión del riesgo, la herramienta se encuentra alineada con el estándar AS/NZ 4360 y la ejecución de auditorías enfocadas hacia la administración del riesgo.

El SOFTAUDIT está basado en el estándar AS/NZ 4360 de la administración del riesgo, como tal se tiene en cuenta las etapas establecidas para la correcta administración del riesgo

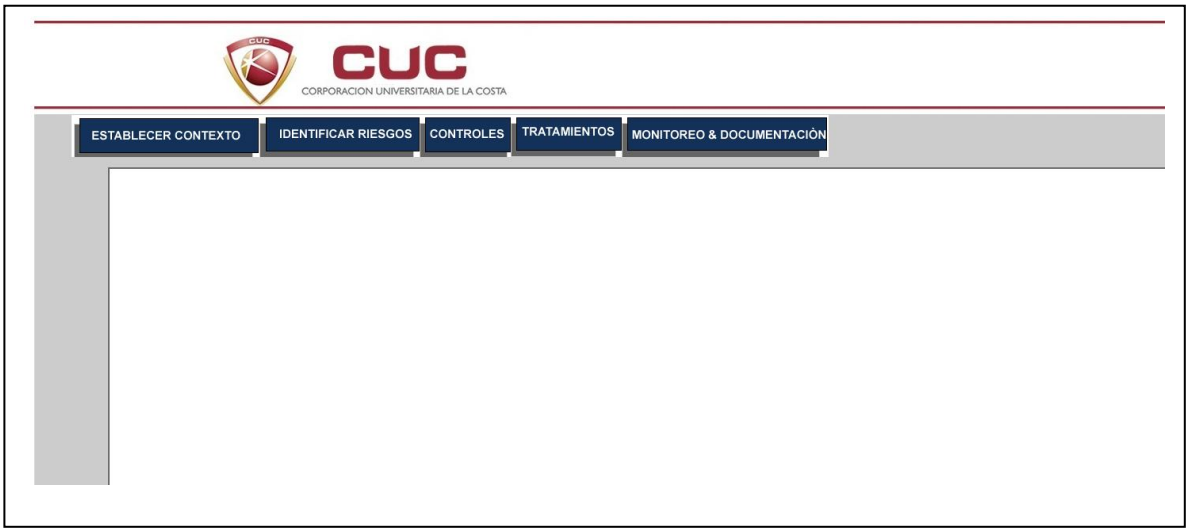


Esta herramienta tiene como objetivo:

- Aplicar el estándar AS/NZS4360, utilizando la metodología AUDAP para facilitar un desempeño eficiente en el área de administración de riesgos.
- Desarrollar un software para dar soporte a la aplicación del estándar 4360 dentro del área de administración de riesgos.
- Implementar el estándar AS/NZS 4360 en conjunto con la metodología AUDAP para facilitar la calidad de toda acción en el área de administración de riesgo.
- Mejorar el proceso de toma de decisiones

CONTENIDO DE SOFTWARE

El software está orientado a web, permitiendo de esta manera que el usuario tenga acceso y también pueda ingresar la información desde cualquier punto, el software tiene un menú en el cual se encuentran 5 opciones, dichas opciones están relacionada con las etapas de la gestión del riesgo definidas por el estándar AS/NZ 4360.



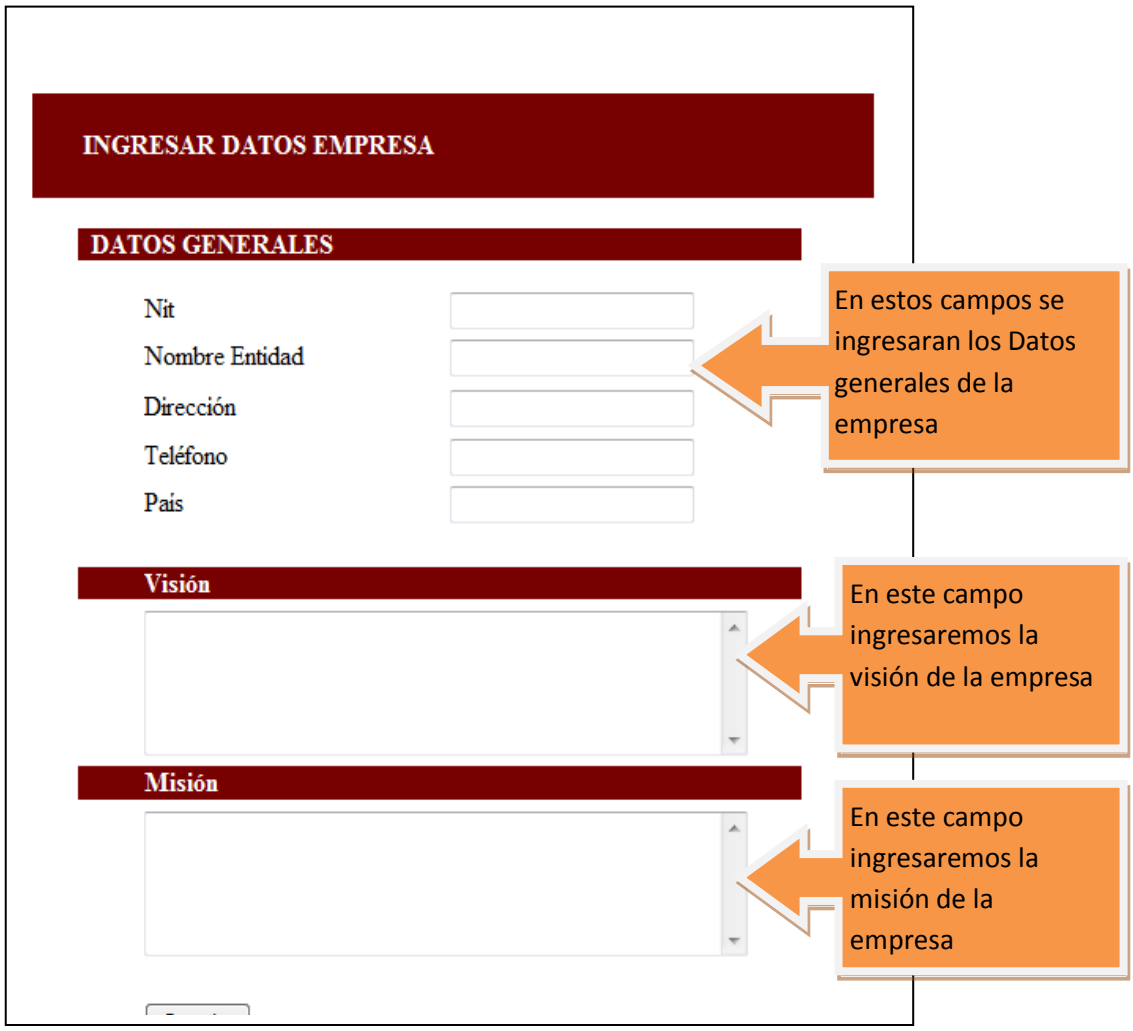
Para la primera etapa de la administración del riesgo, se establecerá el contexto estratégico del área, empresa, proyecto, etc. en el cual trabajaremos, SOFTAUDIT maneja un menú nombrado **ESTABLECER CONTEXTO,** el cual contiene los aspectos a tener en cuenta durante la etapa anteriormente nombrada, este menú está compuesto de la siguiente manera:

- **ESTABLECER CONTEXTO**
  - **Crear nueva empresa**
  - **Ingresar Objetivos Empresa**
  - **Ingresar Metas Empresa**
  - **Contexto Empresarial**
  - **Matriz DOFA**
    - **Ingreso DOFA**
    - **Ver Matriz DOFA**
  - **AREA EMPRESA**
    - **Crear Nueva Área**
    - **Ver Listado de Áreas**
    - **Descripción de Áreas**
  - **PROCESOS**
    - **Crear Nuevo Proceso**
    - **Listado de Procesos**
    - **Descripción de Procesos**

  - **CRITERIOS DE EVALUACION DE RIESGOS**
    - **Probabilidad**
      - **Nuevo Criterio Probabilidad**
      - **Listado de Criterios Probabilidad**
    - **Impacto**
      - **Nuevo Criterio Impacto**
      - **Listado de Impactos**
    - **Niveles de Severidad**
      - **Crear Nivel de Severidad**
      - **Asignar Criterios a Nivel de severidad**
      - **Mapeo**
  - **Áreas de Impacto**
    - **Crear área de impacto**
    - **Ver listado de Áreas de impacto**
  - **Fuentes de Riesgo**
    - **Crear Fuentes de Riesgo**
    - **Listar Fuentes de Riesgo**

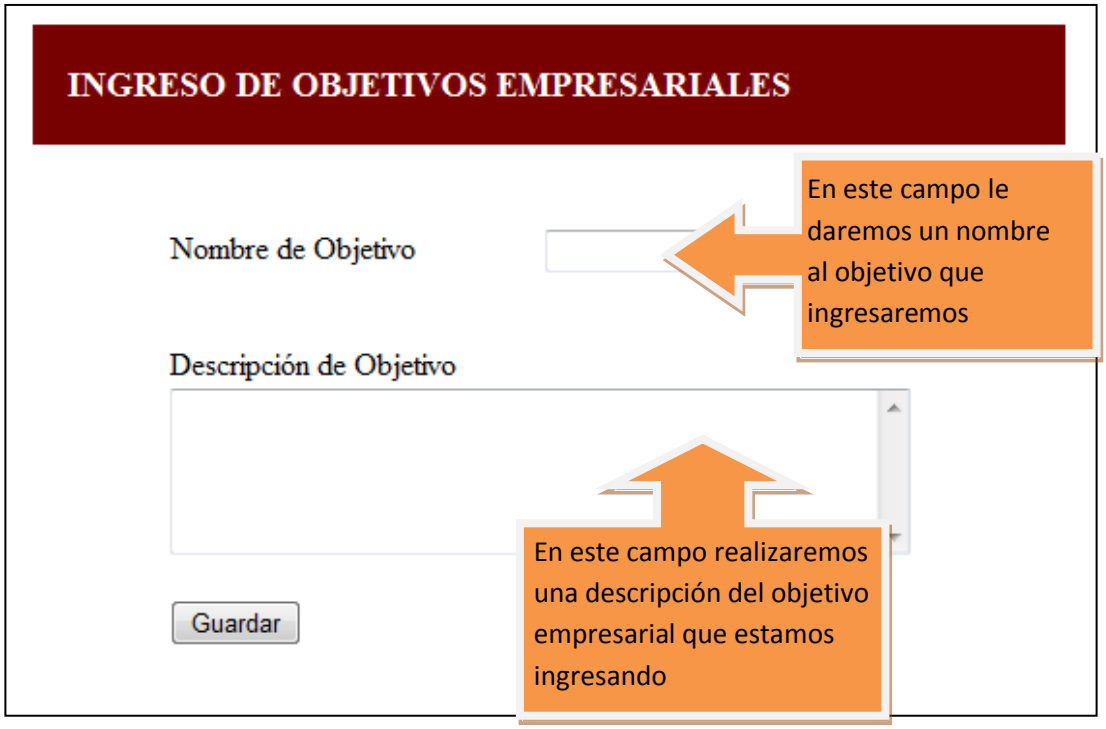
Crear nueva empresa

En esta opción realizaremos la creación de la empresa, definiendo los aspectos básicos de esta:



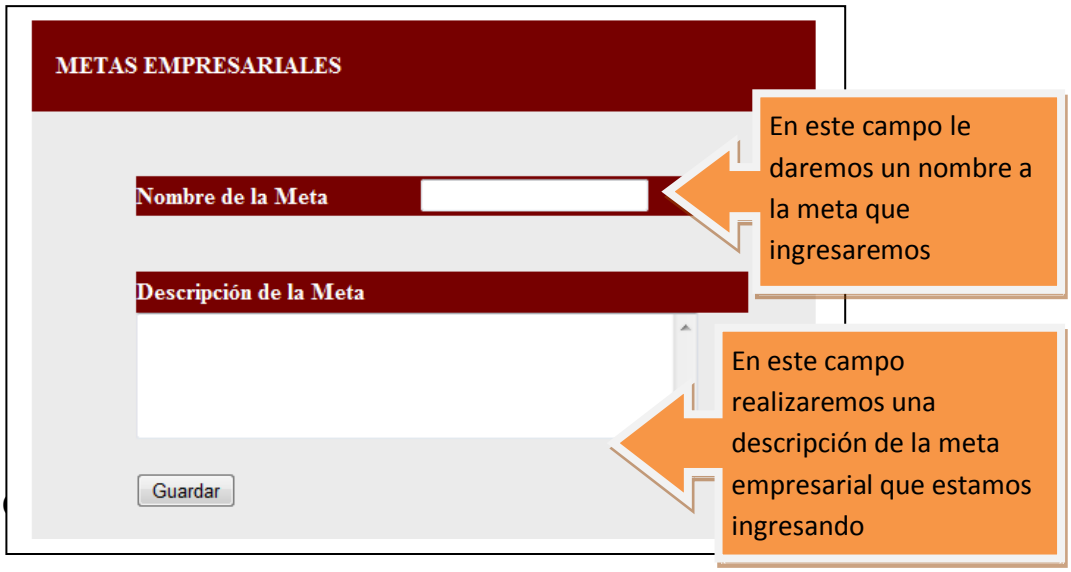
Una vez tengamos la empresa en la cual se realizara la gestión del riesgo, procederemos a continuar con la definición del contexto en el cual trabajaremos, por lo tanto ingresaremos los objetivos que posee la empresa.

Esto lo realizaremos mediante la opción: **ESTABLECER CONTEXTO/Ingresar Objetivo Empresa.**



INGRESAR METAS EMPRESA

En esa opción ingresaremos las metas que tiene la empresa:



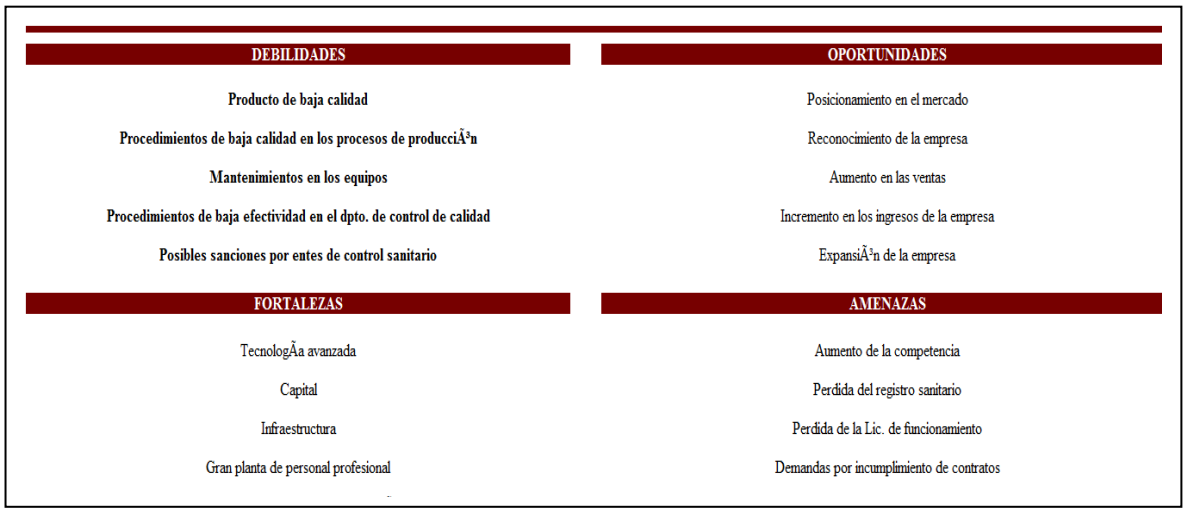
Este es un reporte en el cual podremos apreciar de manera general el contexto que enmarca la empresa en la cual se está realizando la gestión del riesgo.

Este informe nos muestra la consolidación de los datos que ya se han ingresado anteriormente, tales como los datos generales de la empresa, sus objetivos, políticas y metas empresariales.

Matriz dofa

En esta opción realizaremos el ingreso de las DEBILIDADES, OPORTUNIDADES, FORTALEZAS y AMENAZAS que posee la empresa, es decir crearemos la matriz DOFA para la definición del contexto en el cual se trabaja la Gestión del Riesgo.

Así mismo podremos ver como se está construyendo la matriz DOFA mediante la opción ver DOFA.

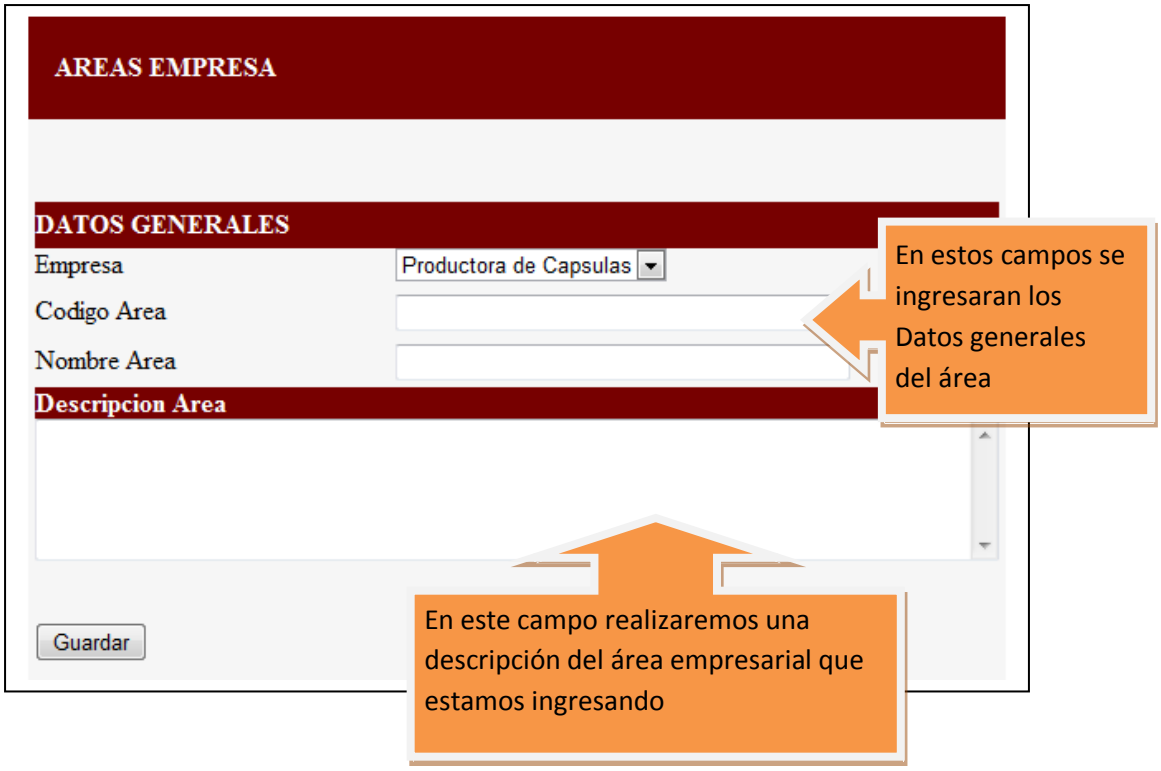


Área empresa

En esta opción Ingresaremos las Áreas que conforman la empresa, en esta opción podremos tanto crear las áreas de la empresa como ver el listado de las áreas que hemos creado junto con su descripción.

Crear Área Empresa

En esta opción crearemos las áreas que conforman la empresa:



Ver Listado de Áreas

Mediante esta opción veremos un listado de las áreas que hemos ingresados junto con su descripción.

Procesos

En esta opción ingresaremos los procesos que conforman las distintas áreas de la empresa en la cual realizaremos la Gestión del riesgo, por tal razón antes de ingresar un proceso, es recomendable que anteriormente se halla ingresado el área en el cual se realiza tal procesos, dado que este formulario se alimenta de las áreas ya ingresadas.

Ver Listado de Procesos

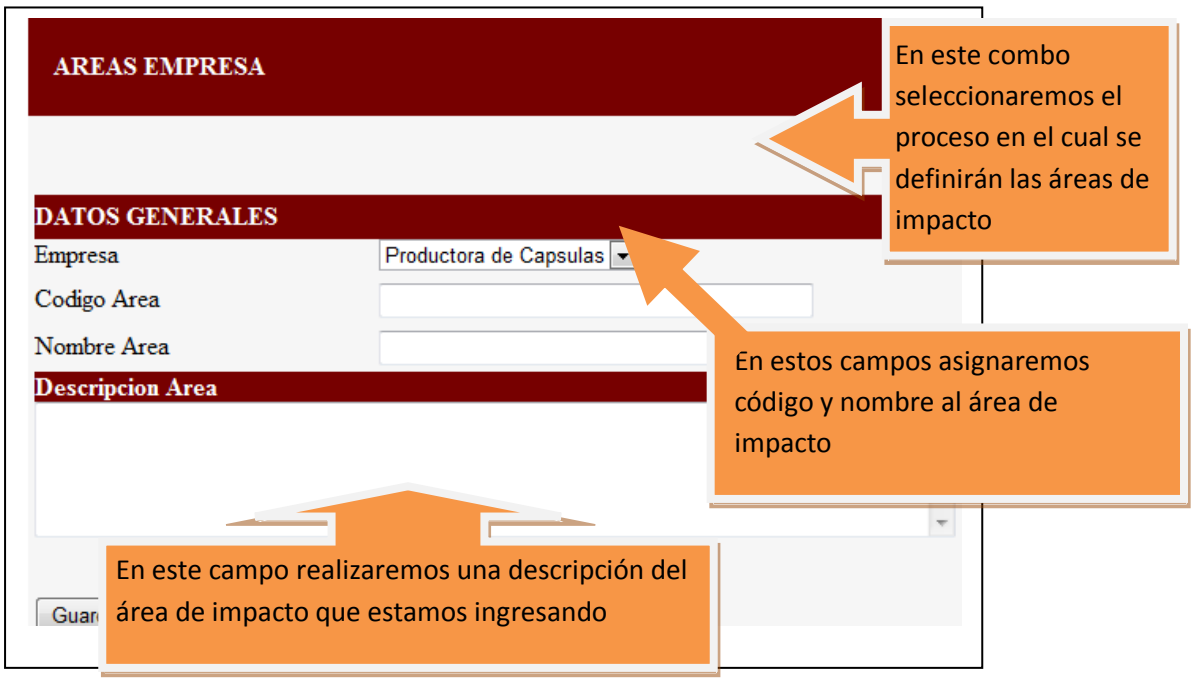
Mediante la opción listado de procesos podremos ver una lista con los procesos que hemos ingresado.

Áreas de impacto

En esta opción ingresaremos las áreas de impacto que se ven afectadas por la materialización de los riesgos.

Crear Área de impacto

Con este formulario crearemos las áreas de impacto que se verán afectadas por la materialización de los riesgos.

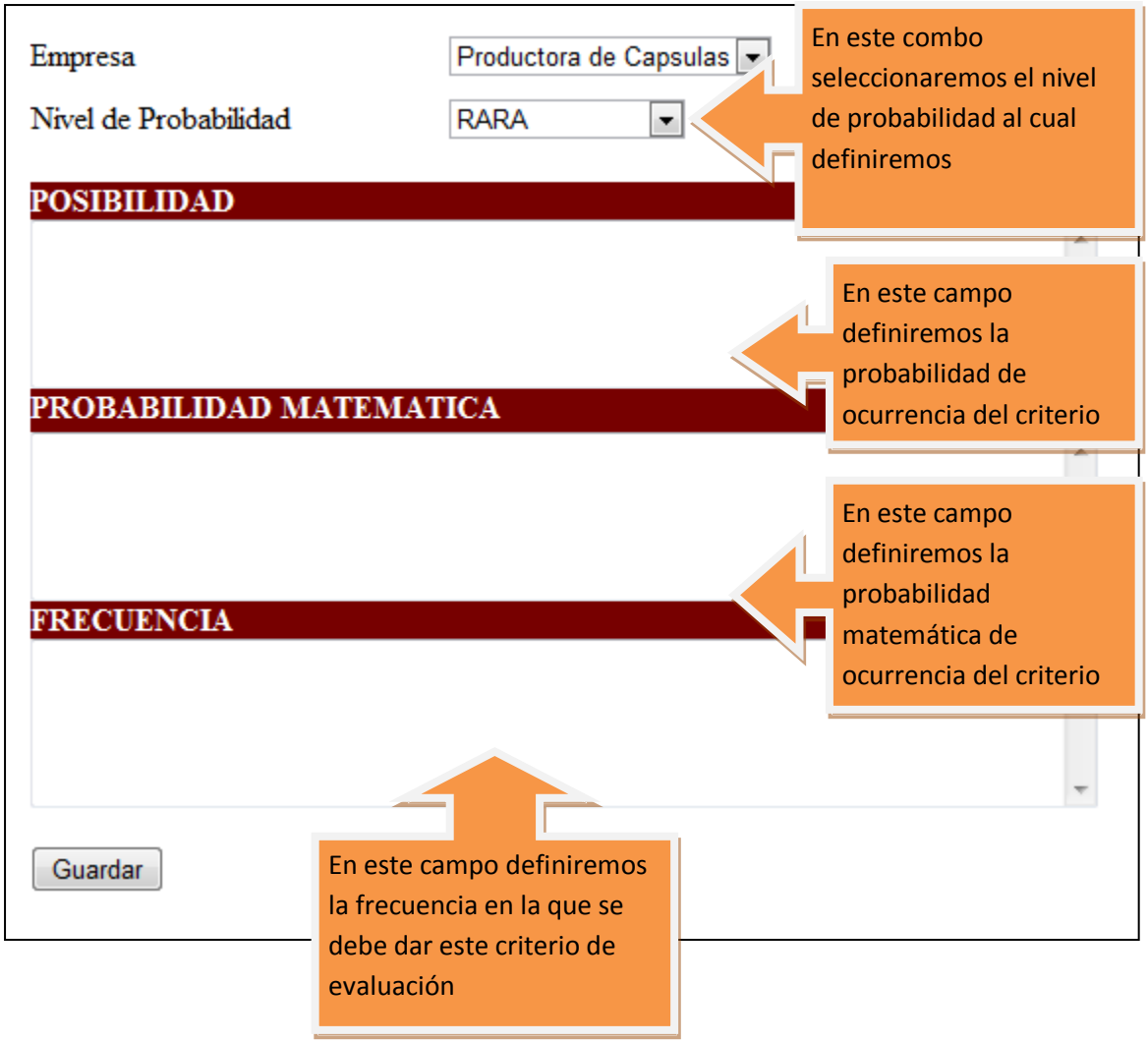


Criterios de evaluación de riesgos

Con esta opción del software podremos ingresar los criterios de evaluación del riesgo, esta opción tiene 2 secciones las cuales son, PROBABILIDAD e IMPACTO.

Las dos primeras opciones son para el ingreso de los criterios de evaluación de los riesgos, mediante la definición de la probabilidad de ocurrencia de los riesgos e impacto a la materialización del riesgo.

Nuevo Criterio de Probabilidad



Listado de Criterios (Probabilidad)

Con esta opción el usuario podrá visualizar los criterios de probabilidad de ocurrencia del riesgo que se están definiendo.

La opción permite ver los criterios organizados de menor a mayor, así como las definiciones de las características a tener en cuenta al momento de evaluar un riesgo.

CRITERIOS DE EVALUACION - PROBABILIDAD DEL RIESGO

CRITERIO	POSIBILIDAD	POSIBILIDAD MATEMATICA	FRECUENCIA	VALOR
RARA	Puede ocurrir en circunstancias excepcionales	Menor a 0.01	Error cada 10.000 operaciones	1
IMPROBABLE	Insignificante posibilidad de que el evento ocurra	>= a 0.01 y < a 0.02	Error cada 1.000 operaciones	2
MODERADA	Alguna posibilidad de que el evento ocurra	>= 0.02 y < a 0.1	Error cada 100 operaciones	3
PROBABLE	Posiblemente ocurra varias veces	>= a 0.1 y < a 0.5	Error cada 10 operaciones	4
CASI CERTERA	Ocurra la mayorÃa de veces	>= a 0.5 y <= a 1.0	Error cada 2 operaciones	5

Nuevo criterio de Impacto

Con esta opción el usuario podrá visualizar los criterios de impacto de ocurrencia del riesgo que se

La opción permite ver los criterios organizados de menor a mayor, así como las definiciones de las características a tener en cuenta al momento de evaluar un riesgo.

CRITERIOS DE EVALUACION - CONSECUENCIA DEL RIESGO

CRITERIO	RECURSOS HUMANOS	PERDIDA ECONOMICA	PERDIDA DE REPUTACION
INSIGNIFICANTE	Sin lesiones o lesiones con incapacidad hasta 3 dias	Hasta $1.000.000	Solo es de conocimiento de los directivos1
MENOR	Incapacidad mayor a 3 dÃas hasta 1 mes	Entre $1.000.001 a $5â€™000.000	De conocimiento de la empresa
MODERADA	Incapacidad mayor a 1 mes hasta 3 meses	Entre $5.000.001 a $50.000.000	De conocimiento a nivel local
MAYOR	Incapacidad mayor a 3 meses hasta 6 meses	Entre $50.000.001 a $500.000.000	De conocimiento a nivel nacional
CATASTROFICA	PÃ©rdida de vidas humanasIncapacidad total y permanente MÃ¡s de 6 meses	Mayores a $500.000.001	De conocimiento a nivel internacional

Una vez hemos terminado con la etapa de definición y establecimiento del contexto en el cual se desarrollara la gestión del riesgo, pasaremos con la siguiente etapa la cual es la identificación, análisis y evaluación de los riesgos presentes en el contexto en el que se llevara a cabo la gestión del riesgo.

En la opción **IDENTIFICAR RIESGOS,** realizaremos las etapas anteriormente mencionadas, el menú está compuesto de la siguiente manera.

- **IDENTIFICAR RIESGOS**
  - Crear Riesgo
  - Asignar Áreas de Impacto
  - Asignar Fuentes de Riesgo
  - Asignar Pues, COMO's y PORQUE's del riesgo
  - Evaluación de Riesgos Absolutos
  - Reportes
    - Listado de Riesgos
    - Descripción de Riesgos
    - Mapeo de Riesgos

Crear Riesgos

El software cuenta con una base de conocimiento, a la cual se le pueden ingresar los nuevos riesgos que identifique el usuario.

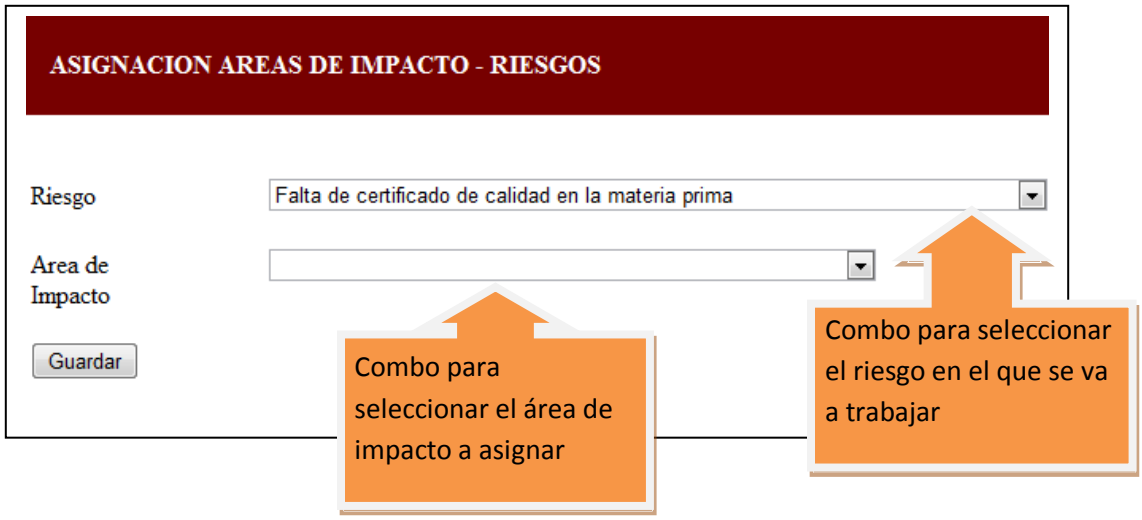
En esta opción el usuario podrá crear nuevos riesgos:

Asignar QUE, COMO y PORQUES del riesgo

Una vez hemos creado un riesgo, el siguiente paso es describir el riesgo, es decir, establecer las fuentes de riesgo y áreas de impacto. El “que puede pasar?” , “Como puede pasar?” y “Porque puede pasar?”, esto se hará en el formulario que se muestra a continuación :

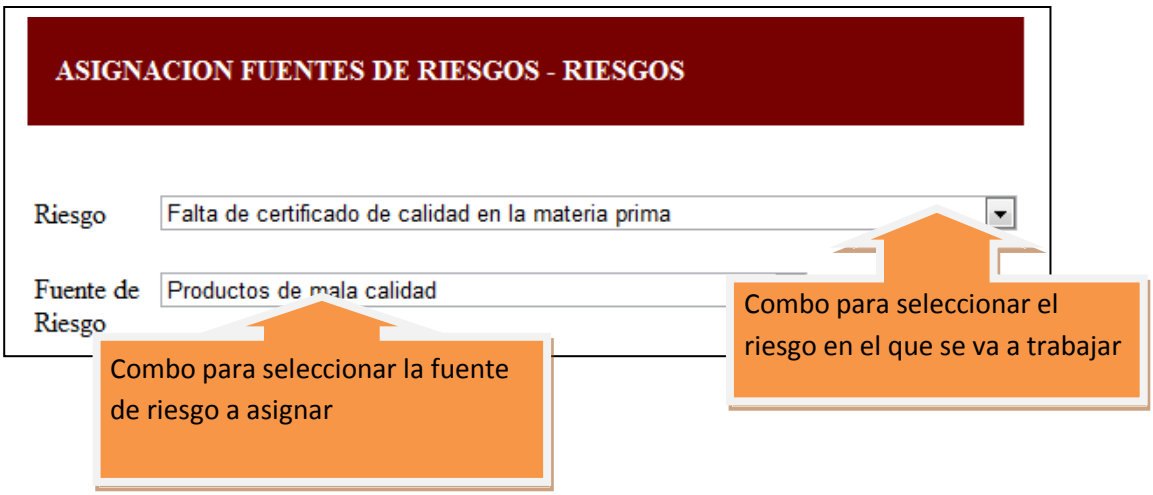
Asignar Áreas de Impacto

En esta opción asignaremos las áreas de impacto previamente ingresadas, a los riesgos que se han creado.

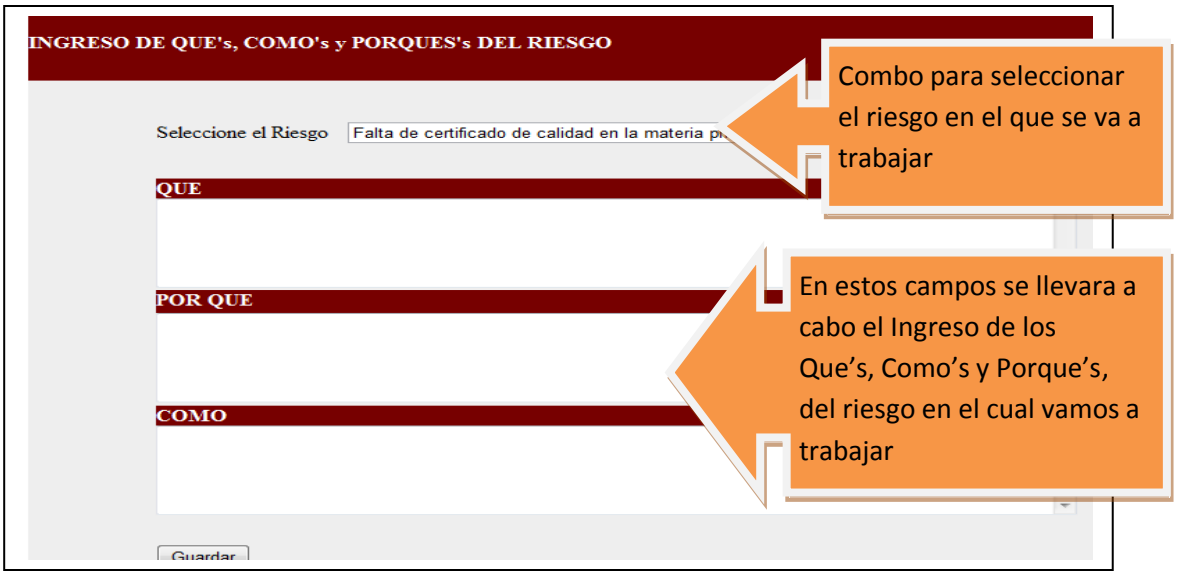


Asignar Fuentes de riesgos

En esta opción asignaremos Fuentes de Riesgos previamente ingresadas, a los riesgos que se han creado.



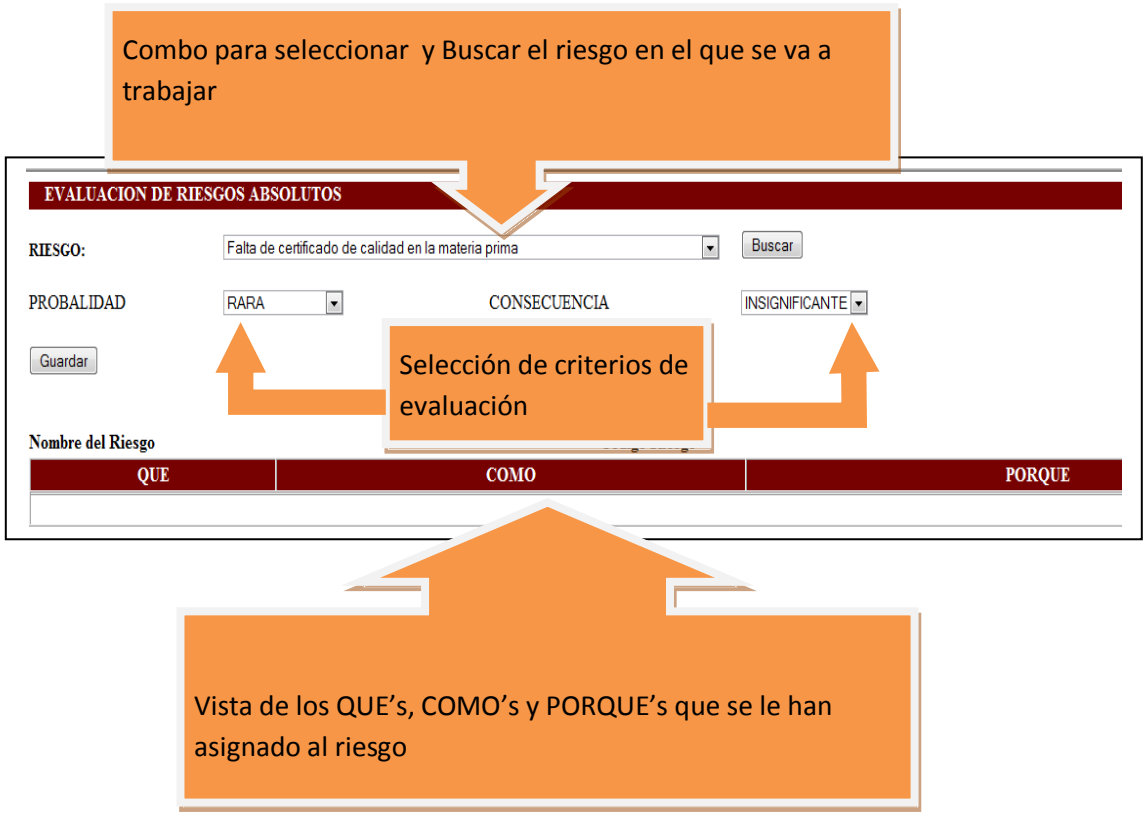
Una vez hemos creado un riesgo el siguiente paso es describir el riesgo es decir establecer el “que puede pasar?” , “Como puede pasar?” y “Porque puede pasar?”, esto se hará en el formulario que se muestra a continuación :



El combo que se muestra en el formulario tiene cargado los riesgos ingresados por el usuario, se deberá escoger el riesgo al cual se le asignaran los QUE's, COMO's y PORQUES's, una vez escogido se mostraran los datos del riesgo como los son el nombre del riesgo, el código del riesgo, área de impacto y fuente de riesgo, esto es para asegurarnos que estamos en el riesgo en el cual se quiere trabajar.

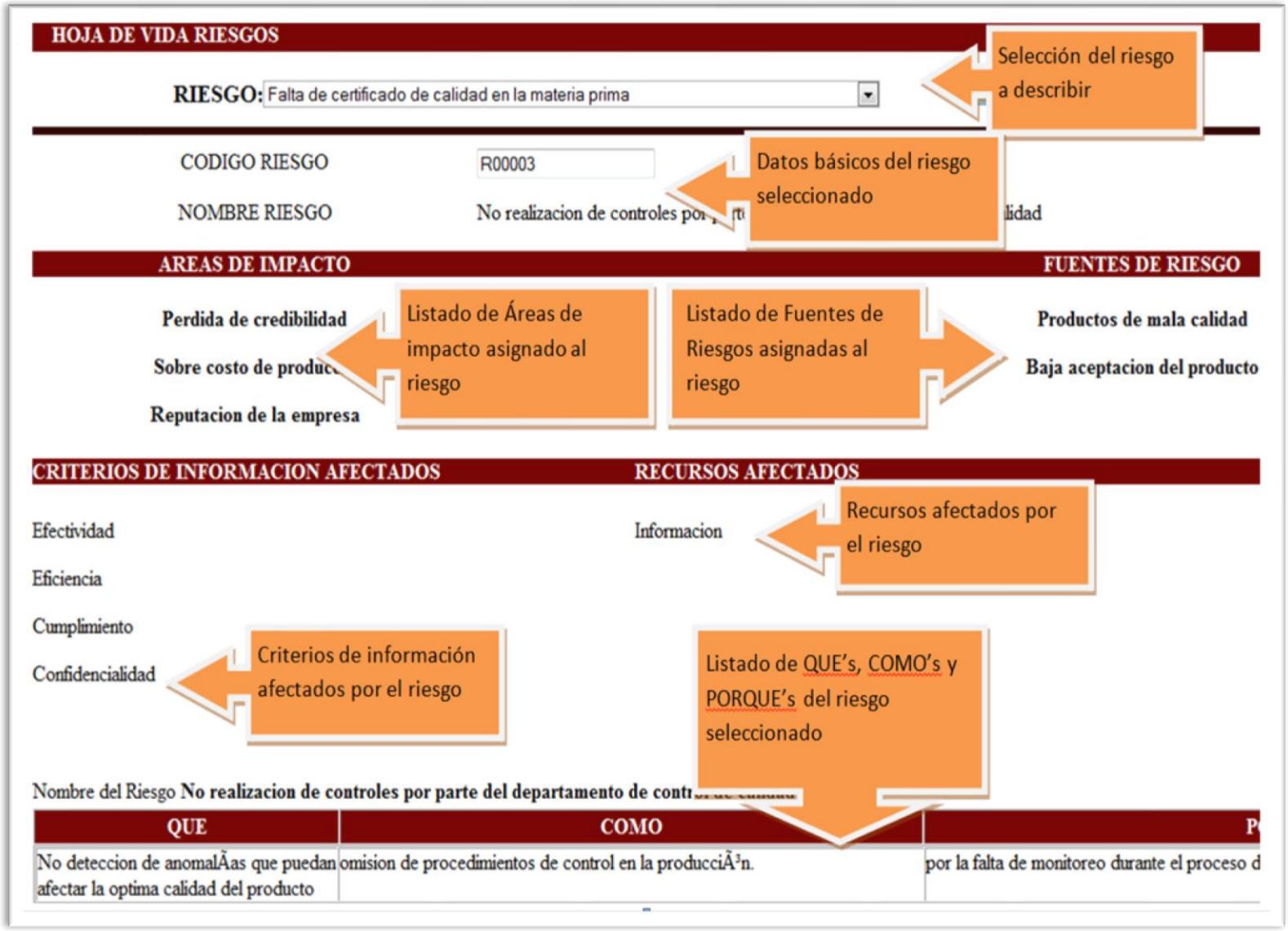
Evaluación de Riesgos Absolutos

En esta opción entraremos a evaluar los riesgos que ya hemos ingresado anteriormente, en la opción **Evaluación de Riesgos Absolutos** podremos realizar esta evaluación, el usuario podrá seleccionar mediante un combo el riesgo a evaluar y podrá ver las diferentes características que se han asignado al riesgo, de esa manera podrá realizar su evaluación de una manera más objetiva.



Reportes

En esta opción encontraremos los reportes de la información que hemos ingresado en el software, tales son listado de riesgos, descripción de los riesgos y mapeo de riesgos.


HOJA DE VIDA RIESGOS
RIESGO: Falta de certificado de calidad en la materia prima
Selección del riesgo a describir
CODIGO RIESGO
R00003
NOMBRE RIESGO
No realizacion de controles por
lidad
Datos básicos del riesgo seleccionado
AREAS DE IMPACTO
FUENTES DE RIESGO
Perdida de credibilidad
Sobre costo de produc
Reputacion de la empresa
Listado de Áreas de impacto asignado al riesgo
Listado de Fuentes de Riesgos asignadas al riesgo
Productos de mala calidad
Baja aceptacion del producto
CRITERIOS DE INFORMACION AFECTADOS
RECURSOS AFECTADOS
Efectividad
Eficiencia
Cumplimiento
Confidencialidad
Informacion
Recursos afectados por el riesgo
Criterios de información afectados por el riesgo
Listado de QUE's, COMO's y PORQUE's del riesgo seleccionado
Nombre del Riesgo No realizacion de controles por parte del departamento de cont
QUE
COMO
P
No deteccion de anomalÃas que puedan afectar la optima calidad del producto
omision de procedimientos de control en la producciÃ³n.
por la falta de monitoreo durante el proceso d

Listado de Riesgos

En este reporte obtendremos una lista de los riesgos que han sido ingresados por el usuario.

LISTADO DE RIESGOS

No	Nombre Riesgo
1	Falta de certificado de calidad en la materia prima
2	Falta de fecha de caducidad
3	No realizacion de controles por parte del departamento de control de calidad
4	Falta de un lugar apropiado para el almacenaje de la materia prima
5	Accidente en la planta de produccion
6	Contratacion de personal no apto para el cargo
7	Ambiente Laboral Inadecuado
8	Carencia de Identificacion de la materia prima
9	Carencia de Orden de produccion
10	Falta de certificado de calidad en la materia prima por parte del proveedor
11	Deficiencia en la planificacion del proceso de producciÃ³n
12	Ausencia de capacitacion de funcionarios para el manejo de software de inventar
13	Perdida del producto por hurto
14	Escases de materia prima

Descripción de Riesgos

En este reporte obtendremos una descripción completa del riesgo que se seleccione, tales como nombre, código, áreas de impacto y fuentes de riesgo, criterios de información afectados y recursos de la empresa y un listado de los QUE’s, COMO’s y PORQUE’s del riesgo seleccionado.

Mapeo de Riesgos

EVALUAION DEL RIESGO ABSOLUTO

RIESGO	PROBABILIDAD	CONSECUENCIA	NIVEL
Transacciones en base de datos con fecha erronea	RARO	Menor	BAJA
Carencia de identificacion de la materia prima	RARO	Menor	BAJA
Perdida de Datos	RARO	Insignificante	BAJA
Contratacion de personal no apto para el cargo	RARO	Insignificante	BAJA

Matriz de Riesgos

El usuario también podrá ver la matriz de riesgos generada a partir de la evaluación de riesgos absolutos.

MATRIZ DE RIESGOS

	INSIGNIFICANTE	MENOR	MODERADA	MAYOR	CATASTROFICA
CASI CIERTA					
PROBABLE					
MODERADA					
IMPROBABLE					
RARA					

Cuando se haya completado las etapas de análisis y evaluación de los riesgos en la opción **IDENTIFICAR RIESGOS,** pasaremos a la siguiente etapa de la gestión de riesgos, la cual es TRATAMIENTOS, la cual se ve reflejada en las opciones:

- CONTROLES
- TRATAMIENTOS

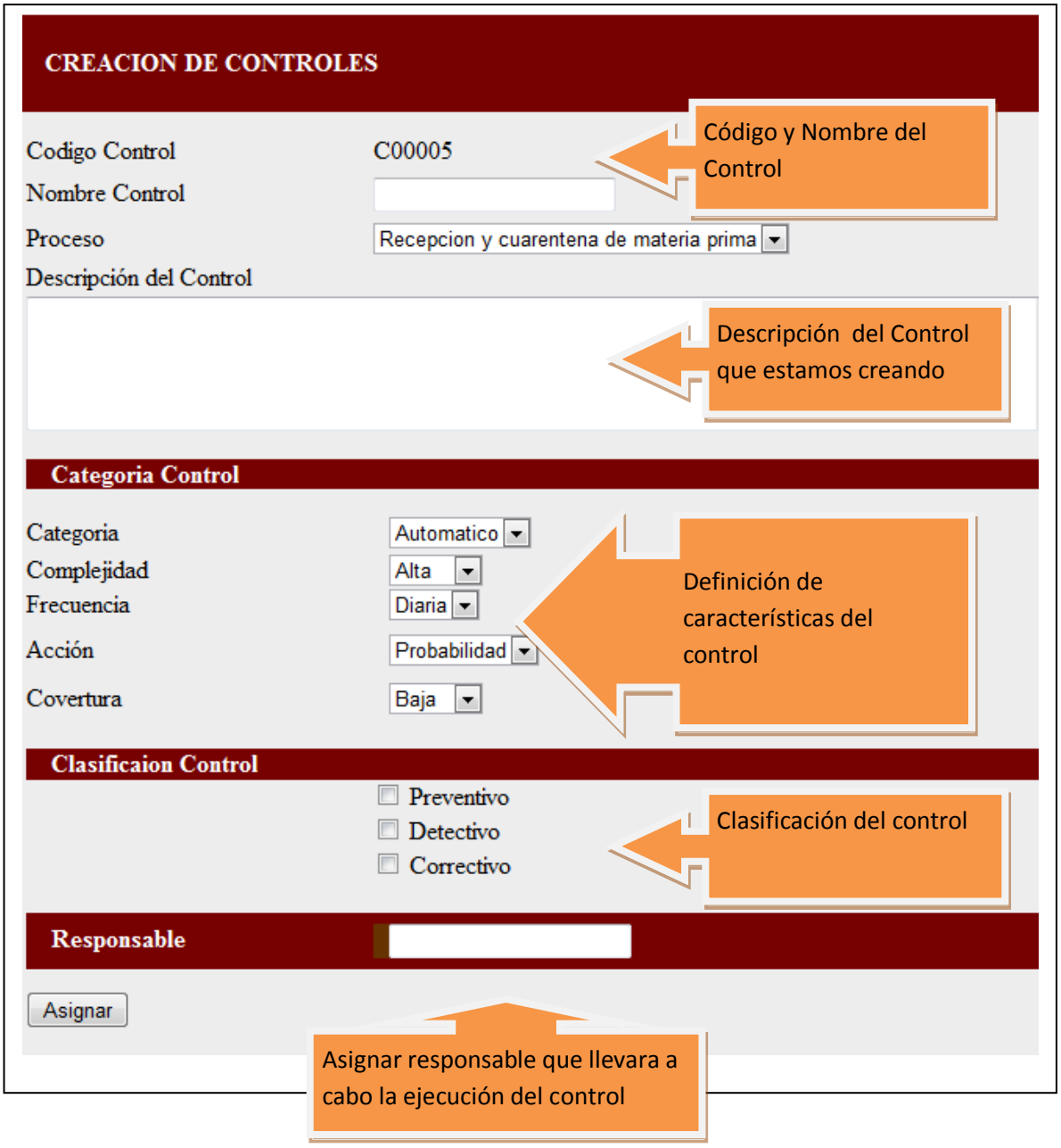
Con estas opciones podremos crear, asignar controles a los riesgos y de la misma manera evaluar los riesgos. También podremos crear, asignar Tratamientos para aquellos riesgos los cuales no fueron aceptados una vez fue evaluado teniendo en cuenta los controles que les fueron asignados.

El menú de CONTROLES se encuentra conformado por las siguientes opciones:

- **CONTROLES**
  - **Crear Control**
  - **Asignar Control a Riesgos**
  - **Evaluación de Riesgos con Controles**
  - **Reportes**
    - **Listado de Controles**
    - **Descripción de Controles**
    - **Mapeo de Riesgos**

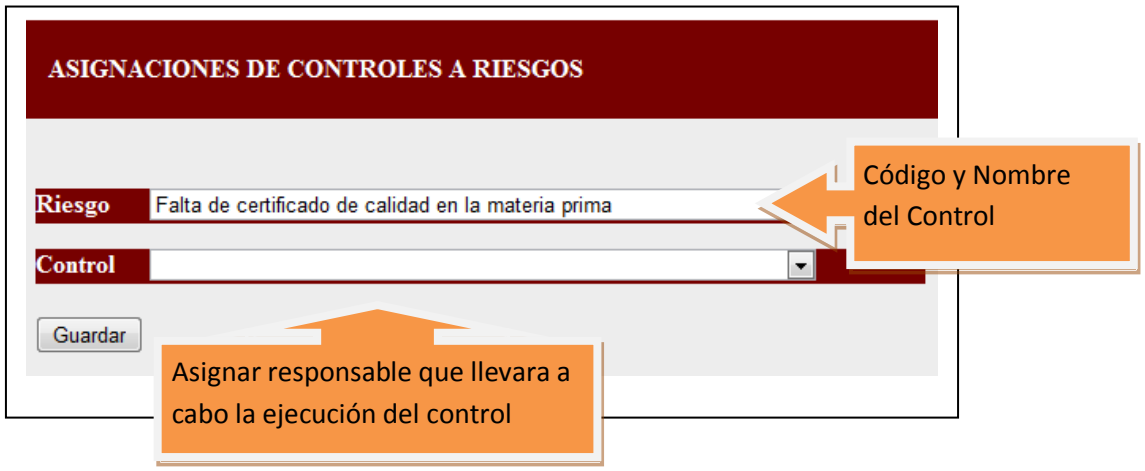
Crear Control

En esta opción podremos crear un control para que luego este sea asignado a un riesgo, dándole un código, nombre y descripción del control, estableceremos las características de este control y clasificaremos el control.



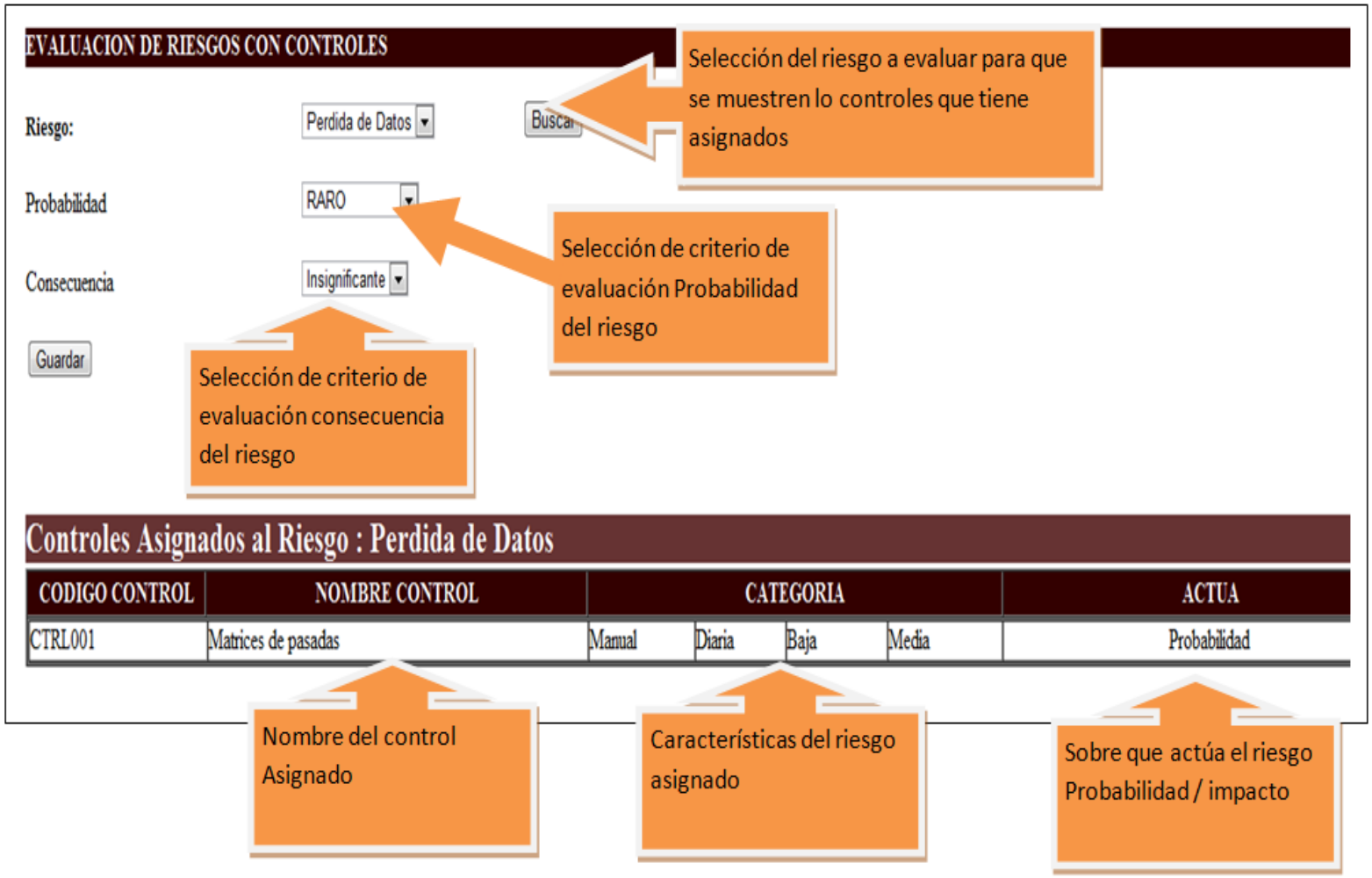
Asignar control a Riesgos

En esta opción asignaremos los controles que ya se han creado, a los riesgos que deseemos.



Evaluación de Riesgos con Controles

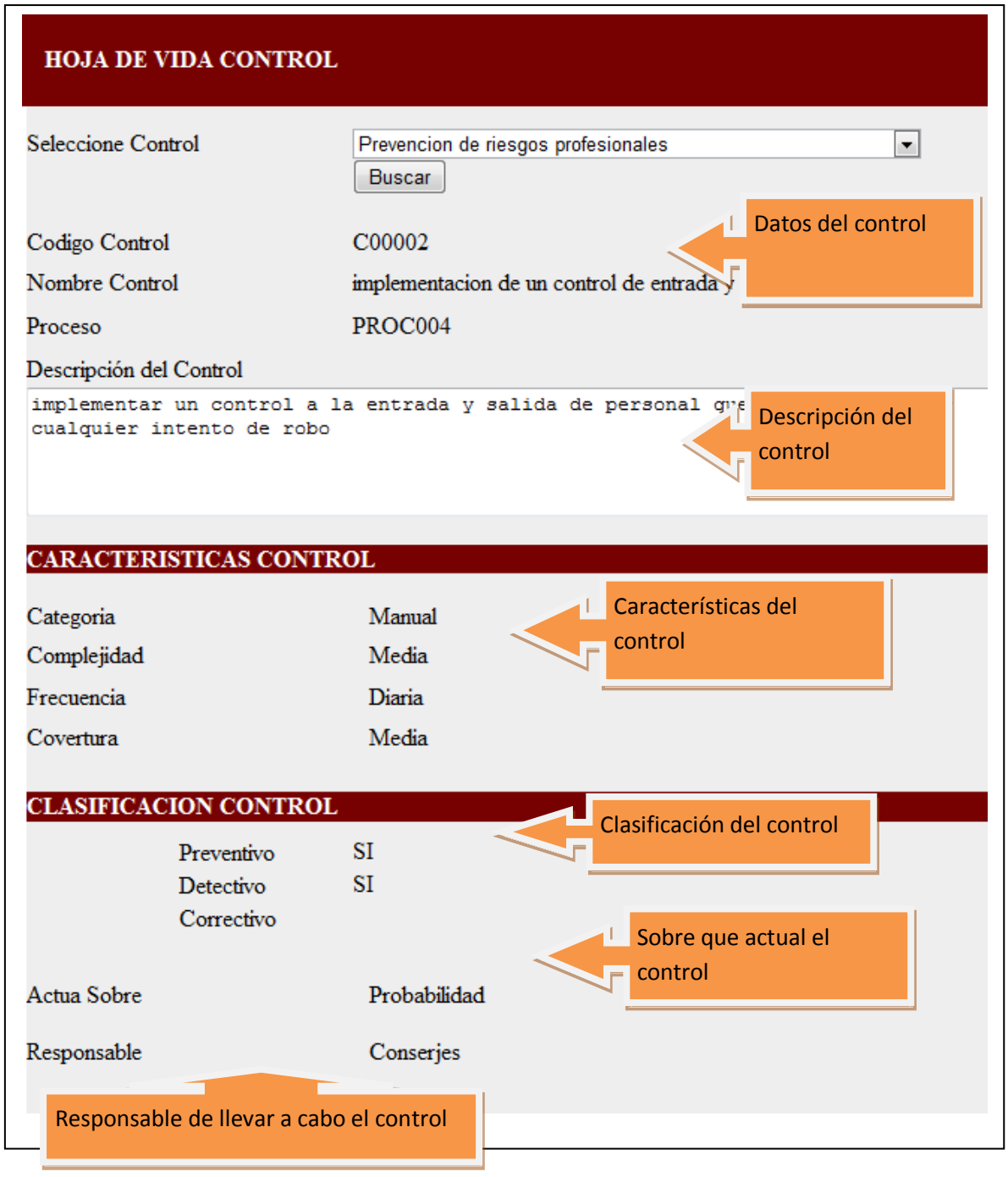
Con esta opción podremos evaluar los riesgos que ya se le han asignado controles, el formulario permite ver que controles han sido asignados a un riesgo en particular, de la misma forma se podrá ver las características del control y si este actúa sobre la probabilidad o el impacto del riesgo, esto es una forma de otorgarle al usuario una forma de identificar las acciones definidas para la mitigación del riesgo y establecer una mejor evaluación del riesgo con los controles asignados.


EVALUACION DE RIESGOS CON CONTROLES
Riesgo:
Perdida de Datos
Buscar
Probabilidad
RARO
Consecuencia
Insignificante
Guardar
Selección del riesgo a evaluar para que se muestren lo controles que tiene asignados
Selección de criterio de evaluación Probabilidad del riesgo
Selección de criterio de evaluación consecuencia del riesgo
Controles Asignados al Riesgo : Perdida de Datos
CODIGO CONTROL
NOMBRE CONTROL
CATEGORIA
ACTUA
CTRL001
Matrices de pasadas
Manual
Diaria
Baja
Media
Probabilidad
Nombre del control Asignado
Características del riesgo asignado
Sobre que actúa el riesgo Probabilidad / impacto

Reportes

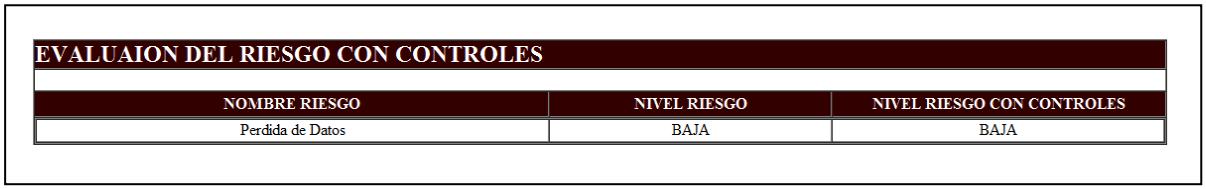
Descripción de Controles

Con este reporte podremos ver de manera detalla las características de un control en particular desde su descripción hasta su clasificación.



Mapeo de Riesgos con Controles

Con este reporte podremos ver el mapa de riesgos evaluados teniendo en cuenta los controles, el reporte muestra la evaluación dada solo teniendo en cuenta el riesgo absoluto y muestra la nueva evaluación teniendo en cuenta los controles.

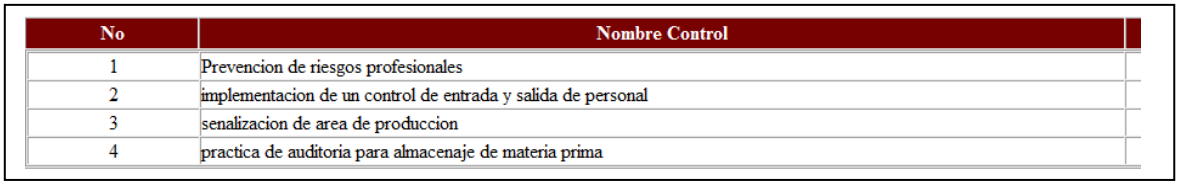


EVALUAION DEL RIESGO CON CONTROLES

NOMBRE RIESGO	NIVEL RIESGO	NIVEL RIESGO CON CONTROLES
Perdida de Datos	BAJA	BAJA

Listado de Controles

En este reporte podremos ver el listado de riesgos creados



No	Nombre Control
1	Prevencion de riesgos profesionales
2	implementacion de un control de entrada y salida de personal
3	senalizacion de area de produccion
4	practica de auditoria para almacenaje de materia prima

Controles Asignados a un Riesgo

En este reporte podremos ver los controles asignados e un riesgo en particular, es decir podremos ver la mezcla de controles que tiene un riesgo.

CONTROLES ASIGNADOS A RIESGOS

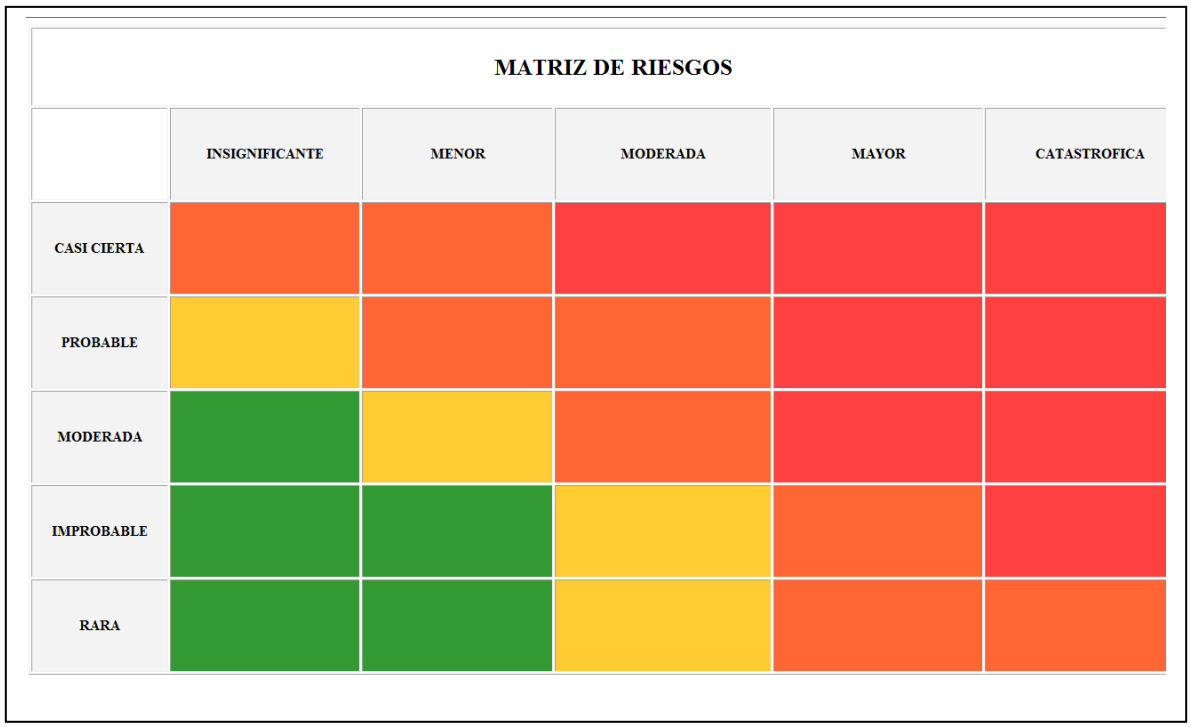
Riesgo: Accidente en la planta de produccion Buscar

Controles Asignados al Riesgo : Accidente en la planta de produccion

CODIGO CONTROL	NOMBRE CONTROL	CATEGORIA	ACTUA

Matriz de Riesgos

El usuario también podrá ver la matriz de riesgos generada a partir de la evaluación de riesgos con Controles



TRATAMIENTOS

- **TRATAMIENTOS**
  - **Crear Tratamiento**
  - **Asignar Elementos a Tratamientos**
  - **Asignar Tratamiento a Control**
  - **Evaluación de Riesgos con Tratamientos**
  - **Reportes**
    - **Listado de Tratamientos**
    - **Descripción de Tratamientos**
    - **Tratamientos Asignados a un Control**
    - **Mapeo Riesgos**

Crear Tratamiento

En esta opción crearemos los tratamientos que luego asignaremos a los controles que los necesiten.

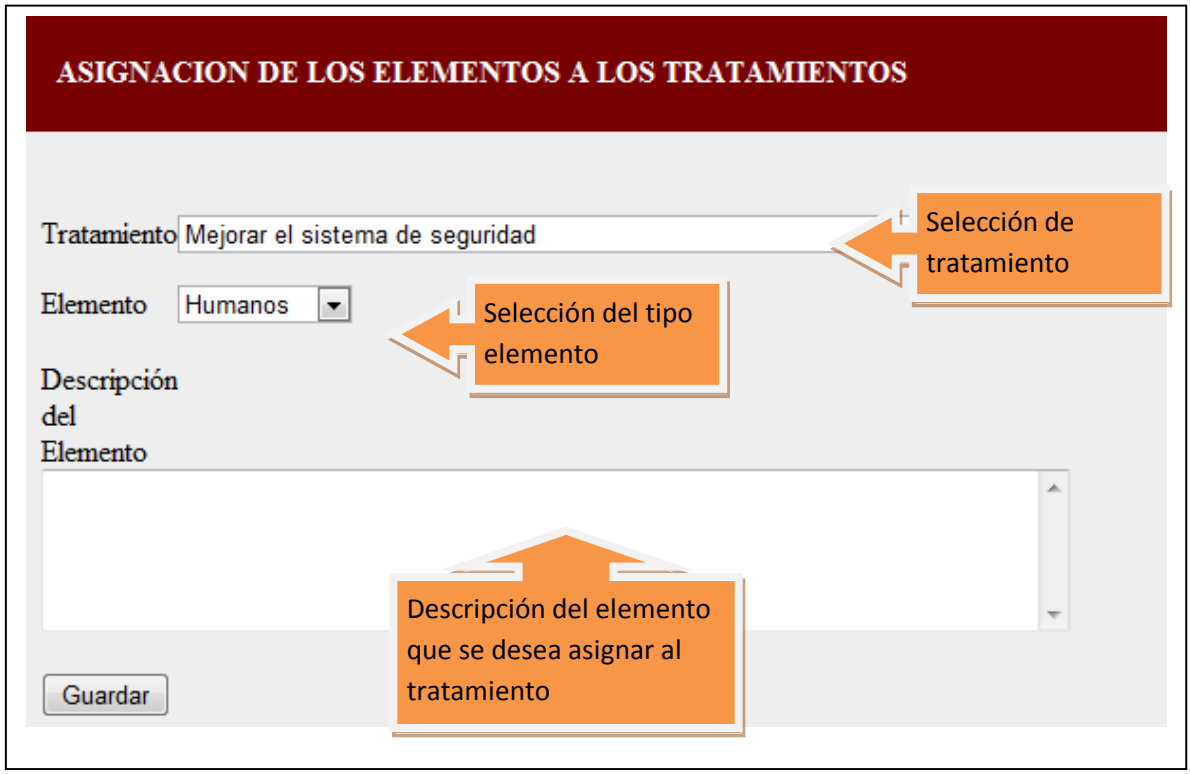
En los datos generales definiremos el riesgo y control sobre los cuales crearemos el tratamiento, estableceremos un código y nombre al tratamiento.

En las características del tratamiento estableceremos las principales características del tratamiento, tales como prioridad, cobertura, Efecto, Estado y el Tipo de tratamiento creado.

Por ultimo estableceremos el propietario del tratamiento, quien será la persona o cargo responsable por llevar a cabo el tratamiento que se está creando.

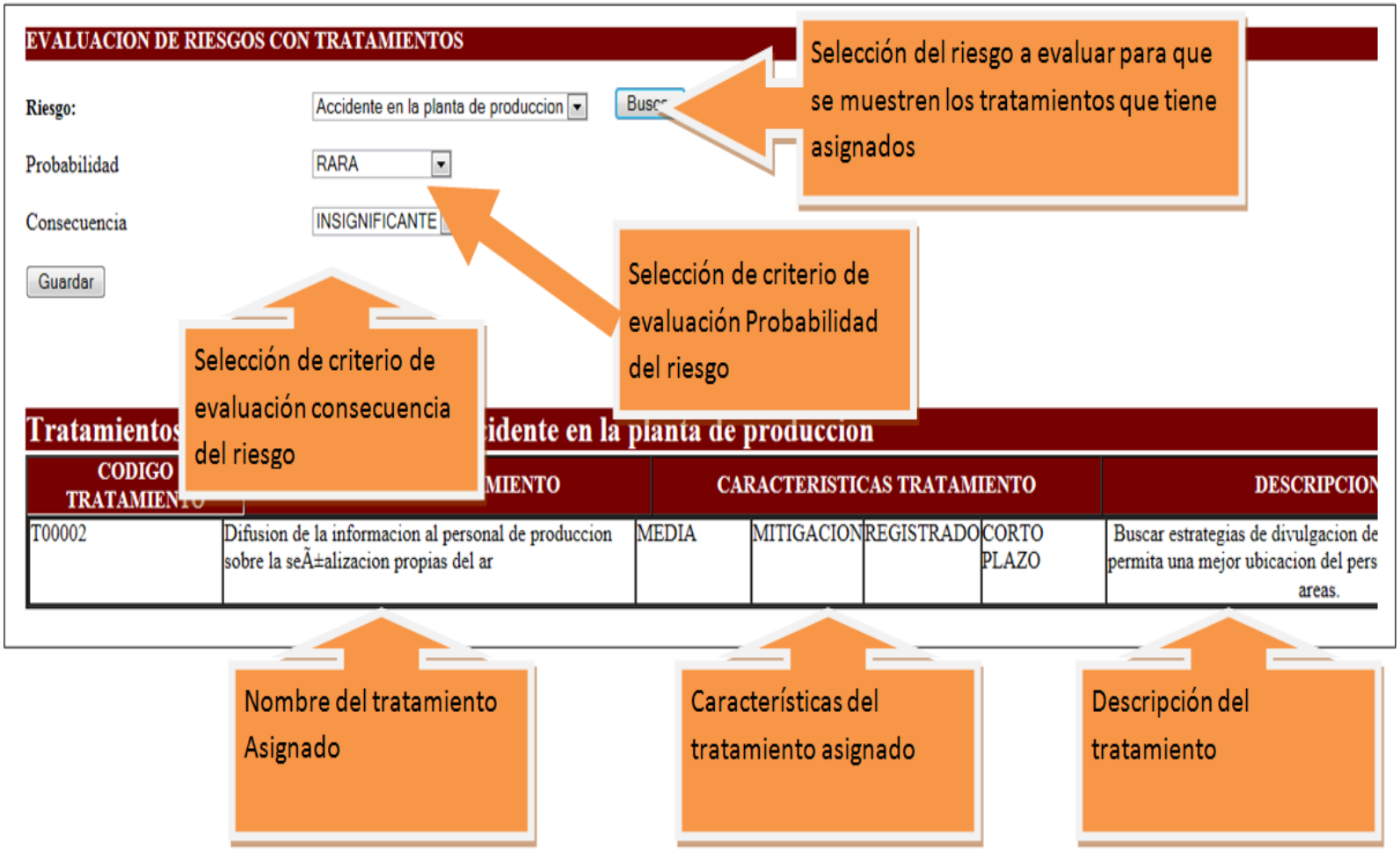
Asignar elementos a tratamiento

Aquí asignaremos los elementos necesarios para llevar a cabo el tratamiento creado, definiremos los elementos según su tipo, ya sean estos HUMANOS, TECNICO o FINANCIEROS, se realizara una descripción del elemento necesario.



Evaluación de riesgos con tratamientos

Con esta opción podremos evaluar los riesgos que ya se le han asignado Tratamientos, el formulario permite ver que tratamientos han sido asignados a un riesgo en particular, de la misma forma se podrá ver las características del tratamiento. Esto es una forma de otorgarle al usuario una forma de identificar las acciones definidas para la mitigación del riesgo y establecer una mejor evaluación del riesgo con los controles asignados.


EVALUACION DE RIESGOS CON TRATAMIENTOS
Riesgo:
Accidente en la planta de produccion
Buscar
Probabilidad
RARA
Consecuencia
INSIGNIFICANTE
Guardar
Selección del riesgo a evaluar para que se muestren los tratamientos que tiene asignados
Selección de criterio de evaluación Probabilidad del riesgo
Selección de criterio de evaluación consecuencia del riesgo
Tratamientos
idente en la planta de produccion
CODIGO TRATAMIENTO
MIENTO
CARACTERISTICAS TRATAMIENTO
DESCRIPCION
T00002
Difusion de la informacion al personal de produccion sobre la seÃ±alizacion propias del ar
MEDIA
MITIGACION
REGISTRADO
CORTO PLAZO
Buscar estrategias de divulgacion de permita una mejor ubicacion del pers areas.
Nombre del tratamiento Asignado
Características del tratamiento asignado
Descripción del tratamiento

Listado de Tratamientos

En este reporte podremos ver los tratamientos que se encuentran creados

Codigo Tratamiento	Nombre Tratamiento	Riesgo Tratado
T00001	Mejorar el sistema de seguridad	Perdida del producto por hurto
T00002	Difusion de la informacion al personal de produccion sobre la seÃ±alizacion propias del ar	Accidente en la planta de produccion

Descripción de tratamientos

con esta opción se podrá ver una descripción detallada del tratamiento que deseamos ver, se podrá apreciar a que riesgo y control se encuentra asignado el tratamiento, así mismo también las características que tiene el tratamiento y los elementos que haces parte de el

Evaluación de riesgos con tratamientos

Este reporte permitirá ver el nivel de severidad en el cual se encuentran los riesgos una vez han sido evaluados teniendo en cuenta los tratamientos que tiene este asignado, el reporte muestra el nivel que obtuvieron en una evaluación anterior (evaluación de riesgos con controles) y al lado mostrara el nivel obtenido con la evaluación de riesgos con tratamientos

EVALUAION DEL RIESGO CON TRATAMIENTOS

NOMBRE RIESGO	NIVEL RIESGO CON CONTROLES	NIVEL RIESGO CON TRATAMIENTOS
Accidente en la planta de produccion	MODERADA	ALTA
Perdida del producto por hurto	MODERADA	BAJA

Matriz de Riesgos

El usuario también podrá ver la matriz de riesgos generada a partir de la evaluación de riesgos con Controles

MATRIZ DE RIESGOS

	INSIGNIFICANTE	MENOR	MODERADA	MAYOR	CATASTROFICA
CASI CIERTA					
PROBABLE					
MODERADA					
IMPROBABLE					
RARA					

9. **CONCLUSION**

Como conclusión tenemos que al realizar el software se obtuvo una herramienta que permite desarrollar de una manera mas eficientes el proceso de administración del riesgo, teniendo como base el estándar AS/NZ 4360, y manejar de una manera mas eficiente la información recolectada durante el proceso.

La metodología asistida por computador AUDAP, permite que la herramienta presente de manera organizada, veraz y eficiente la información para facilitar el proceso de toma de decisiones que se deban realizar a lo largo de la ejecución del proceso de gestión de riesgo en la organización.

Esta herramienta permitirá el eficiente desarrollo de la implementación de un proyecto de gestión de riesgos dentro de una organización

La base de conocimiento con la que cuenta la herramienta permitirá que se aumente el universo de riesgos con los cuales se puede trabajar e ingresar nuevos riesgos, de esta manera el software no se vera limitado a lo existente dentro de su base de datos ni a lo que le alimente del usuario, se podrá combinar estos para crear una base de conocimientos en continuo crecimiento.

La medición de los riesgos se podrá hacer de manera eficiente dado que permitirá visualizar dicha evaluación mediante el uso de matrices de riesgos, las cuales permitirán avistar el grado de impacto que puede causar un riesgo en particular

Se podrá tener acceso de manera rápida y organizada a la información recolectada e ingresada por las actividades creadas, programadas y ejecutadas, el acopio de evidencias se podrá hacer de manera ágil y siempre referenciando la actividad en la cual fueron realizadas y de esta manera al realizar una revisión se podrá tener acceso a estas teniendo en cuenta la actividad en la cual fueron realizadas.

Todo lo anterior en miras de ofrecer una herramienta capaz de contribuir de manera importante al proceso de gestión de riesgos.

10. **CRONOGRAMA DE ACTIVIDADES**

AÑO	**2012**																											
MES	**ENERO**				**FEBRERO**				**MARZO**				**ABRIL**				**MAYO**				**JUNIO**				**JULIO**			
Etapas (Semanas)	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Asesoria Metodológica																												
Documentación																												
Diagnostico inicial																												
Organización del Material																												
Clasificación de información																												
Análisis del Sistema																												
Determinación de requerimientos funcionales																												
Determinación de requerimientos no funcionales																												
Diseño del Software																												
Diseño Base de Datos																												
Desarrollo Base de Datos																												
Pruebas en Base de Datos																												
Diseño de Formularios																												

AÑO	2012																											
MES	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO			
Etapas (Semanas)	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pruebas de formularios con ingreso de datos en BD																												
Análisis de resultados																												
corrección de Errores																												
implementación software																												

BIBLIOGRAFIA

- **COBIT 4.1**
  - Autores : ISACA; IT Governance Institute

- **Reunión Informativa Del Consejo sobre la Gobernabilidad TI**
  - (Board Briefing on IT Governance)
  - Author: IT Governance Institute

- **PROYECTO DE INVESTIGACION I**
  - Author: Gustavo QuevedoGalban

- **DAFP -GUIA DE ADMINISTRACIÓN DEL RIESGO**
  - Autor: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA

- **AUDAP: Metodología Asistida por Computador para auditoría orientada al riesgo en operaciones automatizadas**
  - Autores: AUDISIS **LTDA.** AUDITORES – CONSULTORES

- **Conceptos Estándar AS/NZS 4360**
  - http://www.softexpert.es/norma-asnzs.php
  - http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=47967

- **Un enfoque práctico de gestión de riesgos TI**
    - http://www.escueladecomputacion.net/?p=640
- **Conceptos norma MAGERIT**
    - http://www.csi.map.es/csi/pg5m20.htm

- **AUDAP / AUDIRISK**
    - http://www.catalogodesoftware.com/producto.aspx?pid=1150
    - http://www.audisis.com/productos.html
    - http://00003vs.dev.radiant.net/Folleto_AUDIRISK.pdf
    - http://00003vs.dev.radiant.net/Folleto_CONTROLRISK.pdf

- **ORCA GRC SUITE**
    - http://www.gcpglobal.com/

- **CERO – Control Estratégico de Riesgo**
    - http://www.riesgoscero.com/
    - http://www.slideshare.net/tfase/cero-software-para-gestin-de-riesgo-operativo-y-lavado-de-activo-10291869
- **RISK ADVISOR**
    - http://www.gitltda.com/noticias/RiskAdvisor.pdf